GMP:MPR
F.#2009R01065/OCDETF# NY-NYE-616

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- X

UNITED STATES OF AMERICA

TO BE FILED UNDER SEAL

- against -

Docket No. 09-CR-466(S-4)(BMC)

JOAQUIN ARCHIVALDO GUZMAN LOERA,
also known as "El Chapo," "El Rapido,"
"Chapo Guzman," "Shorty," "El Senor,"
"El Jefe," "Nana," "Apa," "Papa," "Inge"
and "El Viejo,"

Defendant.

- X

MEMORANDUM OF LAW IN OPPOSITION TO THE DEFENDANT'S MOTIONS TO SUPPRESS

RICHARD P. DONOGHUE
UNITED STATES ATTORNEY
Eastern District of New York
271 Cadman Plaza East
Brooklyn, New York 11201

ARTHUR G. WYATT, CHIEF
Narcotic and Dangerous Drug Section
Criminal Division
U.S. Department of Justice

OF COUNSEL:
BENJAMIN G. GREENBERG
United States Attorney
Southern District of Florida

TABLE OF CONTENTS

PRELIMINARY STATEMENT

The government respectfully submits this memorandum of law in opposition to the defendant Joaquin Guzman Loera's motions to suppress (1) the defendant and his coconspirators' telephone calls from the defendant's communications servers located in the Netherlands (the "Dutch Calls"), see Dkt. No. 264; and (2) the defendant and his coconspirators' electronic communications and other data captured by a spyware program known as FlexiSpy (the "FlexiSpy Data"), see Dkt. No. 263. The Court should deny the defendant's suppression motions in their entirety because (1) the motions are untimely; (2) the defendant lacks standing to move to suppress under the Fourth Amendment; and (3) assuming arguendo that the defendant timely filed the motions and that he had standing, the searches to obtain the Dutch Calls and the FlexiSpy Data did not violate the Fourth Amendment.

BACKGROUND

To obtain the Dutch Calls and the FlexiSpy Data, the government relied on the assistance of a confidential source ("CS"). The CS was a computer engineer who designed a private, encrypted communications system used by the defendant and some of his Colombian cocaine suppliers. In approximately 2008, the CS set up an encrypted communications system for a Colombian cartel, which supplied the defendant and the Sinaloa Cartel with large quantities of cocaine (the "Colombian Cartel"). Through his/her contacts with the Colombian Cartel, the CS met the defendant in approximately late 2008. The defendant asked the CS to build him a similar communications system, so that he and other members of the Sinaloa Cartel could communicate with each other. The CS agreed to build this communications network for the defendant. The communications system became operational in approximately 2009 (the "Guzman Network").

I. The Guzman Network

The CS worked for the defendant managing the Guzman Network from approximately 2009 through 2012. During this period, the CS and other members of the Cartel whom the defendant had hired to manage the system had access to the servers on the Guzman Network; such access was necessary to maintain the system and develop new capabilities. The Guzman Network evolved over time, as the CS and other workers added additional capabilities and adapted to new technologies. In essence, the Guzman Network permitted certain members of the Sinaloa Cartel, selected by the defendant, to make encrypted telephone calls and send encrypted text messages to each other, to avoid interception by law enforcement authorities. More specifically, the Guzman Network ultimately consisted of, inter alia: (1) a server that supported external voice communications from Cartel members inside the network to

individuals outside the network, and vice versa; (2) a server that supported internal encrypted voice communications between DTO members using "Voice Over Internet Protocol" ("VOIP");[1] and (3) a server that supported encrypted BlackBerry emails and text messages between Cartel members using BlackBerry handheld devices.[2] Initially, these servers were located in Colombia; the CS, however, subsequently moved them to Mexico and then Canada. Ultimately, as discussed further below, the CS moved the servers to the Netherlands, after the CS started cooperating with U.S. law enforcement. The CS moved these servers with the knowledge of the defendant, who changed the server location as part of his efforts to avoid law enforcement detection of his communications.

II. The FlexiSpy Software

During the period in which the CS created and maintained the Guzman Network, the defendant also asked the CS—prior to him becoming a government source—to provide him with the capability to monitor the communications of several of his girlfriends. In response to this request, the CS purchased numerous licenses for spyware software called FlexiSpy for the defendant, and the CS created usernames and passwords for these accounts.[3]

---

[1] VOIP is one of a family of internet technologies, communication protocols and transmission technologies that allows telephone calls to be routed through the Internet, as opposed to over traditional telephone lines via cellular telephone networks.

[2] A server is a centralized computer that provides services for other computers connected to it via a network or the Internet. The computers that use the server's services are sometimes called "clients." When a user accesses email, Internet web pages or access files stored on the network itself, those files are pulled electronically from the server, where they are stored, and are sent to the client's computer via the network or the Internet. Notably, server computers can be physically located hundreds (or even thousands) of miles away from the client computers.

[3] Spyware is a type of computer program that can be installed on computers, mobile phones and other electronic devices that collect information about the users of the

The CS then installed the spyware on mobile phones and Blackberry handheld devices, which the CS then provided to associates of the defendant, along with the usernames and passwords for the accounts. The defendant then had the devices distributed to his girlfriends and other Sinaloa Cartel members whom he chose to monitor.

The FlexiSpy software collected and stored the following types of data, among others, from the devices on which it was installed: (1) GPS data showing the geographic location of the device over time; (2) toll records and/or call logs for phone calls made from and received by the device; and (3) text messages and/or Blackberry messages sent from or received by the device. This data ultimately was collected and stored by a cloud server controlled by Amazon and located in the United States.[4] Using the spyware, the defendant also could remotely turn on a device's microphone, without knowledge of the device's user, to surreptitiously intercept and listen to live conversations.[5] In short, the defendant could use the spyware, among other things, to monitor the text communications, phone calls and location of the users of the devices on which he had the spyware installed. By February 2012, the CS had purchased dozens of FlexiSpy licenses on the defendant's behalf. Because the defendant regularly communicated with the persons to whom he provided the devices with the FlexiSpy

---

devices without their knowledge. Typically, spyware software is secretly installed on the user's electronic device without his or her knowledge, and it is often very difficult to detect.

[4] Cloud computing is a term for technologies that provide IT services, such as computation, software, data access and storage devices, that do not require the user to know the physical location and configuration of the system that delivers the services. Cloud computing providers deliver software applications to the user via the Internet, while the software itself is stored on cloud servers at a remote location. A user can access the applications through a web browser, as if the programs were installed locally on their own computer or mobile phone.

[5] The Amazon Cloud Server did not collect and store these live communications.

software installed, the defendant's communications with such persons were stored in the Amazon Cloud Server, along with the other data described above. The defendant, in effect, wiretapped himself.

The defendant and/or his associates regularly accessed and monitored the FlexiSpy Data stored on the Amazon Cloud Server. Indeed, the defendant directed one of his workers to monitor the FlexiSpy Data on a regular basis. To access the data, the defendant or his associates would log on to the website of a company called Cloudflare, located in Texas, which handled data retrieval requests for FlexiSpy. The defendant or an associate then would type in the username and password (previously provided by the CS) for the particular device that he wanted to monitor. Cloudflare then retrieved the data stored on the Amazon Cloud Server and sent it to the defendant's computer in a matter of seconds. The data was constantly updated as the spyware collected additional information. As part of his job duties for the defendant, the CS had access to the data collected by the spyware, as did other Cartel members whom the defendant had tasked with monitoring the data for him. At times, the defendant and/or his workers deleted FlexiSpy Data from the Amazon Cloud Server.

III. The Dutch Calls

In approximately February 2011, Federal Bureau of Investigation ("FBI") agents approached the CS, seeking his/her proactive cooperation against the defendant and others. Subsequently, at the direction of the FBI, the CS moved the Guzman Network servers from Canada to the Netherlands. Upon moving the servers to the Netherlands, the CS continued to have access to those servers as part of his/her duties for the defendant; other workers for the defendant also had access. In late March and early April 2011, the government submitted the first in a series of Mutual Legal Assistance Treaty ("MLAT") requests to the

Netherlands.[6] In response to those requests, Dutch authorities obtained judicial authorization to intercept the communications over three separate servers that were part of the Guzman Network, which were identified by their IP addresses.[7] In particular, Dutch authorities obtained judicial authorization to monitor two servers on April 6, 2011. See April 5, 2011 MLAT Request, Ex. A. Interception for the third server began on April 13, 2011. See April 13, 2011 MLAT Request, Ex. B. The Dutch court authorized interception for a period of 30 days on each of the three servers. Shortly thereafter, Dutch authorities began providing the intercepted communications to the FBI.

From April 2011 to December 2011, the government submitted supplemental MLAT requests seeking renewal of the Dutch electronic surveillance on the three servers, for 30 days at a time. During this period, Dutch authorities intercepted hundreds of calls made by high-level members of the Sinaloa Cartel, including calls made by the defendant, his secretary and his brother. Dutch authorities provided these calls to FBI agents on an ongoing basis in response to the government's MLAT requests. Additionally, while the servers were active in the Netherlands in early April 2011, but prior to the beginning of Dutch authorities' electronic

[6] Eighteen MLAT requests related to the Guzman Network are attached hereto as Exhibits A-R, respectively. As noted below, see footnote 13 infra, the government produced unredacted copies of these MLAT requests as part of its 18 U.S.C. § 3500 material for law enforcement officers, disclosed on July 5, 2018. The government is reproducing those materials as exhibits to this motion with Bates numbers 11311A-11334A, 11338A-11340A, 11344A-11360A, 11365A-11370A and 11373A-11375A. The redacted versions of MLAT requests pertinent to this motion, which the government previously produced, are attached hereto as Exhibits A-1, B-1, C-1, D-1, E-1 and J-1.

[7] An Internet Protocol ("IP") address is the number assigned to a network equipped piece of hardware by which other devices identify it.

surveillance, the CS accessed the server directly and recorded calls of the defendant and his coconspirators, which the CS then emailed directly to FBI agents. The FBI obtained the calls directly from the CS at this time to avoid losing the calls while Dutch authorities processed the MLAT request and began electronic surveillance on the servers. The CS again accessed the server directly and emailed recorded calls of the defendant and his coconspirators to FBI agents in late June and early July 2011. At that time, FBI agents had become aware that the interception method utilized by Dutch authorities was not capturing all of the calls passing through the servers. See July 18, 2011 MLAT Request, Ex. G at 11329A-11330A. Again, to avoid losing the calls, the FBI obtained the calls directly from the CS. Due to these technical difficulties, the government requested that Dutch authorities alter their interception method, which the Dutch authorities did. See id. Subsequently, the FBI learned that the computer servers had recorded and stored certain calls between the defendant and his coconspirators. In September and October 2011, the government thus requested that Dutch authorities obtain and execute search warrants on the servers for those calls. See Sept. 12, 2011 MLAT, Ex. J at 11345A-11346A; Oct. 3, 2011 MLAT, Ex. K at 11348A.[8]

Thus, in sum, the government obtained the Dutch Calls by three different methods: (1) Dutch authorities' electronic surveillance; (2) the CS's direct access to the server and (3) Dutch authorities' search warrants. While many of the calls were captured by more than one method, some of the calls were captured by only one of the methods. The defendant was intercepted on several dozen of the Dutch Calls, along with numerous other members of

[8] Dutch authorities' electronic surveillance captured the Dutch Calls in real-time, while their search warrants captured calls that had been previously recorded in the servers.

the Sinaloa Cartel. During those calls, among other things, he discusses trafficking cocaine and methamphetamine into the United States. He also discusses acts of violence committed by members of his Cartel, payments to corrupt police officers and efforts to evade law enforcement detection.

IV. The FlexiSpy Warrants

In approximately August 2011, the defendant stopped using the phones on the Guzman Network set up by the CS and began to rely largely on text messaging (using phones not on the Guzman Network) to communicate with Sinaloa Cartel members.[9] But he continued to use the FlexiSpy software that the CS had obtained for him. From approximately January 2012 to July 2012, FBI agents obtained a series of search warrants (the "FlexiSpy Warrants") to obtain the FlexiSpy Data—i.e., the defendant and his coconspirators' stored electronic communications, as well as location and other data—from the Amazon Cloud Server.

Primarily at issue on this motion are the first three FlexiSpy Warrants, which the government obtained on January 6, 2012 ("FlexiSpy Warrant I"), January 30, 2012 ("FlexiSpy Warrant II") and February 16, 2012 ("FlexiSpy Warrant III").[10] See Exs. S-U,

[9] Other members of the Cartel continued using the Guzman Network's servers in the Netherlands. Interception of the Guzman Network terminated on January 9, 2012. The CS also set up servers in the Netherlands that members of the Colombian Cartel, who were close associates of the defendant, used to communicate. During 2012, the government submitted MLAT requests to obtain calls from those servers, and the CS directly emailed some of those calls to FBI agents as well.

[10] The government obtained additional FlexiSpy Warrants on the following dates: February 18, 2012 ("FlexiSpy Warrant IV"); February 23, 2012 ("FlexiSpy Warrant V"); February 24, 2012 ("FlexiSpy Warrant VI"); March 13, 2012 ("FlexiSpy Warrant VII"); June 18, 2012 ("FlexiSpy Warrant VIII"); June 25, 2012 ("FlexiSpy Warrant IX"); June 27, 2012 ("FlexiSpy Warrant X"); June 28, 2012 ("FlexiSpy Warrant XI"); June 29, 2012 ("FlexiSpy Warrant XII"); July 18, 2012 ("FlexiSpy Warrant XIII"); July 25, 2012 ("FlexiSpy Warrant XIV") and August 1, 2012 ("FlexiSpy Warrant XV"). FlexiSpy Warrants IV-XV are

respectively. As set forth in FlexiSpy Warrant I, in approximately December 2011, FBI agents consulted with representatives of Cloudflare and Amazon regarding whether those companies could execute search warrants for the FlexiSpy Data. See Ex. S at 12147A. As a result of those consultations, the FBI agents learned that Cloudflare did not possess the data and "that due to the nature of how cloud servers store the data, it would be extremely difficult, and potentially impossible, for Amazon to locate the requested data, even with the usernames and passwords for the accounts." Id. Thus, although Amazon had possession of the data, it could not provide it to the FBI in response to the search warrant. See id.

On December 22, 2011, at the direction of FBI agents, the CS "logged into the FlexiSpy website, accessed the spyware accounts using the usernames and passwords (which he had retained after purchasing the licenses), and downloaded all of the text messages, Blackberry messages, call logs/toll records, GPS location data, and other data onto an Amazon server owned by the FBI." Id. at 12147A-12148A.[11] After several days, on December 29, 2011, FBI agents then downloaded the files onto a DVD, which they stored at the FBI's New York Field Division office, within the Southern District of New York ("SDNY"). See id. at 12148A; Dec. 29, 2011 Chain of Custody Form, Ex. HH. Thereafter, on January 6, 2012, FBI agents obtained FlexiSpy Warrant I to search the DVD. The FBI repeated this process in advance of FlexiSpy Warrant II, when the CS downloaded data on January 29, 2012. See Ex. T at 12187A. The FBI agents obtained FlexiSpy Warrant II on the following day. See id. at

---

attached hereto as Exhibits V-GG, respectively. The redacted versions of FlexiSpy Warrants I-III, which the government previously produced, are attached hereto as Exhibits S-1, T-1 and U-1, respectively.

[11] The CS discussed herein is referred to as "CS-2" in the FlexiSpy Warrants.

12189A. Notably, both applications cited United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001), stating that, in that case, "the Government had employed a similar method, under analogous circumstances, to collect data in order to execute a search warrant, which the District Court found appropriate." Ex. S at 12148A; Ex. T at 12186A.

The government changed its method for obtaining the data in FlexiSpy Warrant III, after learning that the previous downloads had not captured Blackberry Messages ("BBMs"), which the CS had stated the defendant typically used to communicate. That search warrant thus sought "authorization for [the] CS[] or the FBI agents to access the Amazon Cloud Server directly, via the Cloud Flare website, rather than downloading the data onto a DVD, as was done with the two prior search warrants." Ex. U at 12227A n.6. The warrant form identified "The FlexiSpy Accounts Listed in Attachment A" as the property to be searched, and it identified the Western District of Washington, where Amazon's headquarters is located, as the location of the property. Ex. U at 12212A. Attachment A to the warrant form listed 35 FlexiSpy accounts "controlled by Amazon and stored on the Amazon Cloud Server," and it directed law enforcement officers to "identify and copy the information contained" in those accounts, which was "authorized to be further copied by this search warrant; namely":

> [T]hose text messages, Blackberry messages, other electronic communications, call logs/toll records, GPS location data, and other data that, from the law enforcement personnel's review (with the assistance of an interpreter, if necessary), based on the content of the communications or date, appear to be pertinent to the trafficking of narcotics or the laundering of drug proceeds.

Id. at 12214A. The warrant application form specifically designated the statutes associated with the offenses for which the officers had probable cause to search, i.e., 21 U.S.C. §§ 959

and 963. Id. at 12216A. The affidavit in support of the warrant similarly identified those statutes, stating there was "probable cause to believe" that the designated FlexiSpy accounts contained "evidence and instrumentalities of violations of" those statutes. Id. at 12218A; see 12231A (same).[12]

In addition to the warrant authorizing the search of the FlexiSpy accounts, FlexiSpy Warrant III also included a separate warrant, submitted simultaneously, authorizing the government to track the "Location Data Contained in the FlexiSpy Accounts Listed in Attachment A." Id. at 12262A, 12266A. The affidavit in support of the tracking warrant application, as well as Attachment A to the tracking warrant form, were identical to those documents submitted in support of the warrant to search the FlexiSpy accounts. Id. at 12264A-12265A. Only the warrant form and warrant application form differed. Id. at 12262A, 12266A. Like the warrant application form to search the FlexiSpy accounts, the tracking warrant application form also designated the statutes associated with the offenses, i.e., 21 U.S.C. §§ 959 and 963. Id. at 12266A. The warrant form designated the Clerk of Court as the person to whom the warrant must be returned. Id. at 12262A.

In terms of establishing probable cause, FlexiSpy Warrants I-III largely relied upon information provided by the CS. Specifically, the warrants detailed the CS's involvement in setting up the Guzman Network and purchasing the FlexiSpy licenses, as well as the CS's understanding, based on conversations with other Sinaloa Cartel members, that the devices associated with the FlexiSpy accounts would be used to discuss drug trafficking. See, e.g., id.

[12] FlexiSpy Warrants III-VII contained identical language in Attachment A and the supporting documents. See Exs. U-Y. FlexiSpy Warrants VIII-XV used different language in Attachment A, specifically listing the statutes at issue in that attachment. See Exs. Z-GG.

at 12271A-12277A. While FlexiSpy Warrant I relied almost exclusively on CS information, see Ex. S at 12142A-12148A, FlexiSpy Warrant II also relied on GPS location data recovered as a result of FlexiSpy Warrant I, see Ex. T at 12186A, while FlexiSpy Warrant III relied on GPS data and the defendant's coconspirators' communications recovered pursuant to FlexiSpy Warrants I &II, see Ex. U at 12228A-12230A. FlexiSpy Warrants IV-XV continued to rely on CS information, including new information from the CS as it developed. See, e.g., FlexiSpy Warrant XV, Ex. GG at 13209A-13242A. Those warrants also relied on the defendant and his coconspirators' communications recovered as a result of earlier warrants, other sources of information and corroborative information observed by law enforcement authorities during capture operations for the defendant. See, e.g., id.

As a result of these search warrants, among other things, the government obtained months' worth of text communications between the defendant and his coconspirators. In that FlexiSpy Data, the defendant discusses trafficking drugs into the United States and other countries. He also discusses narrowly escaping Mexican authorities' raid of one of his residences in Cabo San Lucas, Mexico in approximately February 2012.

*****

On July 9, 2018, the defendant filed motions to suppress the Dutch Calls and the FlexiSpy Data. For the reasons discussed below, the Court should deny those motions in their entirety.

ARGUMENT

I. The Defendant's Motions Are Untimely

The defendant's suppression motions, which he filed three months after the court-imposed April 9, 2018 motion deadline, are untimely. During the February 15, 2018 status conference, the Court set a deadline of April 9, 2018 by which the defendant was to file his pretrial motions. See Tr. of Feb. 15, 2018 Status Conf. at 7:13-15 ("That [April 9 deadline] will apply to defendant as well, as to all motions that could reasonably have been made based on information turned over prior to that date."); Dkt. No. 193 (setting April 9, 2018 deadline for defendant's motions). Following that deadline, at the June 26, 2018 status conference, the defendant informed the Court that he intended to file a motion to suppress. See Tr. of June 26, 2018 Status Conf. at 15:24-25. In response, the Court directed the defendant to file his motion within ten days and stated that the defendant must "demonstrate in that motion, and any others, that [he] could not reasonably have been expected to make it earlier based on the information that [he] had." Id. at 16:24-17:4. The defendant's motions to suppress, however, do not rely on any new facts, information or evidence not available to the defense prior to the deadline set by this Court. Indeed, the government produced copies of the MLAT requests and FlexiSpy Warrants—on which the defendant relies in his motions—at least five months prior to this April 9, 2018 deadline. See Dkt. No. 119, 165. On this basis alone, the Court should deny the defendant's motions. See United States v. Moore, 541 F. Appx. 37, 39 (2d Cir. 2013) ("A district court may grant relief from an untimely motion upon a showing of: (1) cause for the defendant's non-compliance, and (2) actual prejudice arising from the waiver." (internal quotation marks omitted)).

In arguing otherwise, the defendant claims that he did not have access to unredacted copies of documents that he needed to file his motion until after the Court's motion deadline. Specifically, with respect to the Dutch Calls, the defendant states that he did not obtain unredacted copies of the MLAT requests from the government to the Netherlands until July 5, 2018. See Dkt. No. 264 at 2 & n.2. He further claims that, "[d]uring the continuing review of discovery, the defense became aware of evidence seized by the government without a warrant." Id. at 2. As for the FlexiSpy Data, the defendant asserts that the government produced unredacted copies of the FlexiSpy Warrants in June and July 2018. See Dkt. No. 263 at 2. He claims that "[i]t was not until the defense was able to fully review the unredacted documents that it became evident that this motion to suppress must be filed." Id. at 2 n.2. The defendant's purported explanations for his late filing are insufficient.

Prior to the motion deadline, the defendant possessed sufficient information to make his motions to suppress. The government produced the redacted copies of its MLAT requests to the Netherlands on August 11, 2017 and November 7, 2017. See Dkt. Nos. 119, 165. It produced redacted copies of the FlexiSpy Warrants on August 11, 2017. See Dkt. No. 119. The government redacted these documents to protect the identities of the confidential sources discussed therein. But the government did not redact information necessary for the defense to evaluate whether to file a motion to suppress. For instance, the redacted MLAT requests disclosed that (1) the government had requested Dutch law enforcement authorities to conduct electronic surveillance of and search warrants related to the communications of the defendant and his coconspirators; (2) Dutch authorities obtained judicial approval in the Netherlands for such surveillance and searches; (3) Dutch authorities, in fact, obtained the defendant's communications; and (4) Dutch authorities shared those communications with the

FBI. See, e.g., Exs. A-1, B-1, C-1, D-1, E-1, J-1. These are the primary facts on which the defendant relied in his motion to suppress the Dutch Calls. See Dkt. No. 264 at 7-9. Similarly, the redacted FlexiSpy Warrants disclosed (1) that the spyware software captured defendant and his coconspirators' communications, see, e.g., FlexiSpy Warrant XV, Ex. GG-1 at 13216-42; (2) that the FBI had directed those communications to be downloaded to a disc prior to obtaining FlexiSpy Warrants I & II, see, e.g., Ex. S-1 at 12147-48; Ex. T-1 at 12187; (3) for FlexiSpy Warrant III and the subsequent warrants, the specific accounts that the government sought to search, see, e.g., Ex. U-1 at 12214; Ex. GG-1 at 13202; and (4) the venue of FlexiSpy Warrant III and the subsequent warrants, see, e.g., Ex. U-1 at 12212; Ex. GG-1 at 13200. These are the primary facts on which the defendant relied in his motion to suppress the FlexiSpy Data. See Dkt. No. 263 at 7-15.

In an effort to justify his delay based on the government's redactions of the FlexiSpy Warrants, the defendant claims that, "[b]ecause Mr. Guzman did not know that CS2 operated on behalf of the government, Mr. Guzman could not have filed a motion contesting the warrantless search and seizure of the servers before receiving the unredacted versions." Dkt. No. 263 at 2 n.2. Not so. While the government redacted references to the CS in its initial production of the FlexiSpy Warrants, the redacted versions still made plain that the FlexiSpy Data was downloaded onto the discs "at the direction of FBI agents," which is the fact on which the defendant relies in his suppression motion. See Ex. S-1 at 12147; Dkt. No. 263 at 7. Similarly, the defendant claims that "the redacted version did not reveal that Mr. Guzman owned the encrypted communications network set up by CS2." Dkt. No. 263 at 2 n.2. The redacted version did, however, indicate that the FlexiSpy licenses were purchased "at the request of [the defendant]" and that the government obtained his communications pursuant to

the FlexiSpy Warrants, see Ex. S-1 at 12141; Ex. T-1 13216-41, facts on which the defendant relies to argue that he had an expectation of privacy in the FlexiSpy Data, see Dkt. No. 263 at 9. Thus, the defendant's contention that the government's redactions deprived him of the information necessary to move to suppress the FlexiSpy Data is unavailing.

Despite possessing the necessary information for more than five months in advance of the April 2018 motion deadline, the defendant did not file his motions to suppress. The defendant did not even raise the possibility of filing a motion to suppress intercepted communications with the government until mid-May 2018—more than one month after the motion deadline had passed. Moreover, even if the government had redacted some relevant information from the FlexiSpy Warrants, the defendant did not even request unredacted copies of the FlexiSpy Warrants until May 22, 2018—over a month after the deadline to file had passed. Likewise, the defendant did not even request unredacted copies of the MLAT requests for the Dutch Calls until July 8, 2018—the day before the court-imposed July 9 deadline to file his motions to suppress. The government provided unredacted copies of these documents to the defendant following his requests, in light of his stated intention to move to suppress the intercepted communications derived therefrom.[13] Thus, in advance of the motion deadline, the defendant could have reviewed the FlexiSpy Warrants and MLAT requests, decided which motions he intended to file and/or made appropriate requests to the government or the Court for unredacted versions of those documents.

[13] In response to his July 8, 2018 request, the government notified the defendant that it had already provided him with unredacted copies of the MLAT requests, as part of its production of 18 U.S.C. § 3500 material for law enforcement officers on July 5, 2018.

The defendant could have—and should have—filed his motions to suppress prior to the court-imposed April 9 deadline. At a minimum, he should have moved to suppress based on the information available to him in the redacted documents in advance of the deadline. Because he did not file any motion to suppress before the filing deadline, despite possessing the information necessary to do so, the Court should deny his motions as untimely. See Moore, 541 F. Appx. at 39 (holding that "lawyer's belated identification of issue cannot constitute cause affording relief" for untimely suppression motion). Regardless, for the reasons set forth below, if the Court proceeds to the merits of his motions, the Court should still deny them.

II. The Defendant Lacks Standing to Move to Suppress under the Fourth Amendment

The defendant claims that he has standing under the Fourth Amendment to move to suppress the Dutch Calls and the FlexiSpy Data. See Dkt. No. 263, 264. The Supreme Court's decision in United States v. Verdugo-Urquidez, 494 U.S. 259 (1990), however, forecloses that argument. Moreover, even if it did not, the defendant has failed to meet his burden to show the type of substantial and voluntary connection to the United States necessary to establish standing pursuant to Verdugo-Urquidez. Thus, as the defendant lacks standing, the Court should deny his suppression motions in their entirety.

A. The Supreme Court's Decision in *Verdugo-Urquidez* Forecloses the Defendant's Motion

Under the Supreme Court's decision in Verdugo-Urquidez, the defendant does not have standing to move to suppress pursuant to the Fourth Amendment. In that case, Mexican authorities arrested the defendant in connection with the murder and torture of Drug Enforcement Administration ("DEA") Special Agent Enrique Camarena Salazar in Mexico. See 494 U.S. at 262. Mexican authorities then handed over the defendant—who was "one of

the leaders of a large and violent organization in Mexico that smuggles narcotics into the United States"—to U.S. authorities at the border. Id. Subsequently, DEA agents requested that Mexican authorities search the defendant's properties in Mexico; during the searches of those properties, Mexican authorities recovered incriminating documents, which the government then sought to introduce at trial against the defendant. See id. The defendant moved to suppress. See id. at 263. Reversing the lower courts' decisions suppressing the evidence, the Supreme Court held that the defendant could not invoke the Fourth Amendment and seek suppression of the evidence. See id. at 261.

In reaching this conclusion, the Court began its analysis by observing that the Fourth Amendment "operates in a different manner than the Fifth Amendment," which "is a fundamental trial right of criminal defendants." Id. at 264. "Although conduct by law enforcement officials prior to trial may ultimately impair that right, a constitutional violation occurs only at trial." Id. "The Fourth Amendment functions differently." Id. "It prohibits unreasonable searches and seizures whether or not the evidence is sought to be used in a criminal trial, and a violation of the Amendment is fully accomplished at the time of an unreasonable governmental intrusion." Id. (internal quotation marks omitted). Thus, with respect to the case at issue, "if there were a constitutional violation, it occurred solely in Mexico." Id. The Court stated that "[w]hether evidence obtained from [the defendant's] Mexican residences should be excluded at trial in the United States is a remedial question separate from the existence vel non of the constitutional violation." Id.

Turning to the text of the Fourth Amendment, the Court then examined the limitations of the Amendment's protections. The Amendment states that it is "'the right of the people to be secure in their person, houses, papers, and effects, against unreasonable searches

and seizures.'" Id. at 265 (emphasis added) (quoting U.S. Const. amend. IV). "That text, by contrast with the Fifth and Sixth Amendments, extends its reach only to 'the people.'" Id. "[T]he people," the Court stated, "seems to have been a term of art employed in select parts of the Constitution." Id. "While this textual exegesis is by no means conclusive, it suggests that 'the people' protected by the Fourth Amendment, and by the First and Second Amendments, and to whom rights and powers are reserved in the Ninth and Tenth Amendments, refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community." Id. "The language of these Amendments contrasts with the words 'person' and 'accused' used in the Fifth and Sixth Amendments regulating procedure in criminal cases." Id. at 265-66.

Next, examining the historical background of the Fourth Amendment, the Court reached the same conclusion with respect to the limits of its protections: "What we know of the history of the drafting of the Fourth Amendment also suggests that its purpose was to restrict searches and seizures which might be conducted by the United States in domestic matters." Id. at 266. "The available historical data show, therefore, that the purpose of the Fourth Amendment was to protect the people of the United States against arbitrary action by their own Government; it was never suggested that the provision was intended to restrain the actions of the Federal Government against aliens outside of the United States territory." Id.

With these principles in mind, and in light of its past precedent, the Court held "that aliens receive constitutional protections when they have come within the territory of the United States and develop substantial connections with this country." Id. at 271; accord Zadvydas v. Davis, 533 U.S. 678, 693 (2001) ("It is well established that certain constitutional protections available to persons inside the United States are unavailable to aliens outside of

our geographic borders."). As the defendant was "an alien who has had no previous significant voluntary connection with the United States," the Court concluded that he was not entitled to such constitutional protections. Verdugo-Urquidez, 494 U.S. at 271. Moreover, the Court rejected the contention that the defendant's "lawful but involuntary" presence in the United States at the time of the search gave rise to "any substantial connection with our country."[14] Id. The Court noted that "the applicability of the Fourth Amendment to the search of premises in Mexico should [not] turn on the fortuitous circumstance of whether the custodian of its nonresident alien owner had or had not transported him to the United States at the time the search was made." Id. at 272. In short, the Court held that the defendant "had no voluntary connection with this country that might place him among 'the people' of the United States." Id.; accord D.C. v. Heller, 554 U.S. 570, 580 (2008) (citing with approval Verdugo-Urquidez's holding that "the people" as used in Constitution refers to "class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community" (internal quotation marks omitted)).

In the wake of Verdugo-Urquidez, lower courts have consistently held that foreign citizens with no substantial voluntary connection to the United States cannot invoke the Fourth Amendment to challenge a search conducted abroad, even if U.S. law enforcement is involved in the search. See, e.g., United States v. Gasperini, No. 16-CR-441 (NGG), 2017 WL 3038227, at *7 (E.D.N.Y. July 17, 2017), aff'd, No. 17-2479-CR, 2018 WL 3213005 (2d

[14] The Court reserved decision on the extent to which a defendant subsequently "might claim the protection of the Fourth Amendment" based on searches conducted after his arrival in the United States, "if the duration of his stay in the United States were to be prolonged—by a prison sentence, for example." Id. at 271-72.

Cir. July 2, 2018) ("The Fourth Amendment does not apply to searches abroad that target persons, such as Defendant, who lack substantial or voluntary connections to the United States. This is the case even where the search is conducted directly by U.S. agents."); United States v. Defreitas, 701 F. Supp. 2d 297, 304 (E.D.N.Y. 2010) (holding that Fourth Amendment "inapplicable" to non-U.S. citizen searched outside country); United States v. Fantin, 130 F. Supp. 2d 385, 390 (W.D.N.Y. 2000) ("[U]nless Defendant can show that prior to the challenged search, . . . he had come within the territory of the United States and established a significant voluntary connection with the United States[,] the Fourth Amendment does not apply to the search even assuming FBI involvement." (internal quotation marked omitted)).

In addition, courts also have held that such foreign citizens cannot invoke the Fourth Amendment to challenge a search conducted by U.S. authorities within the United States. See, e.g., United States v. Gutierrez-Casada, 553 F. Supp. 2d 1259, 1265 (D. Kan. 2008) ("Cases decided after Verdugo-Urquidez have applied its 'sufficient connection' approach even to searches occurring within the United States."); United States v. Esparza-Mendoza, 265 F. Supp. 2d 1254, 1273 (D. Utah 2003) (holding that previously deported felon found within United States "lack[ed] sufficient connection to this country to assert a Fourth Amendment suppression claim").

Recognizing this legal hurdle to his motion to suppress, the defendant asserts that he has sufficient connections to the United States to invoke the Fourth Amendment. See Dkt. No. 264 at 9-10. Specifically, he claims that, because the government has alleged that the defendant ran the Sinaloa Cartel, which imported tons of heroin, cocaine, methamphetamine and marijuana, "the government itself alleges that [the defendant] has

substantial and voluntary connections to the United States." Dkt. No. 264 at 10. Under Verdugo-Urquidez, however, the Court should reject this argument.

As discussed above, in Verdugo-Urquidez, the Court concluded that a large-scale Mexican drug trafficker (who, like the defendant, was a member of the Guadalajara Cartel, the predecessor to the Sinaloa Cartel) lacked sufficient contacts with the United States to invoke the Fourth Amendment. See 494 U.S. at 261-62. It reached this conclusion, despite the government's allegations that the defendant was "one of the leaders of a large and violent organization in Mexico that smuggles narcotics into the United States." Id. at 262. Accordingly, under Verdugo-Urquidez, the defendant's "participation in a drug trafficking conspiracy directed at importing drugs into the United States does not mean that he was part of the 'national community' protected by the Fourth Amendment." United States v. Emmanuel, 565 F.3d 1324, 1331 (11th Cir. 2009). Indeed, as a foreign citizen, living abroad, who dedicated his entire adult life to poisoning American streets, the defendant cannot reasonably be considered one of "the people" of the United States; rather, he was a foreign threat to them.

Thus, at the time of the relevant searches in 2011 and 2012, the defendant was "entirely outside" the "national community" protected by the Fourth Amendment. Id. The defendant has not established that, at the time of the searches, he had "come within the territory of the United States" and established the type of substantial connection necessary to invoke the Fourth Amendment. 494 U.S. at 259; see Fantin, 130 F. Supp. 2d at 390-91 (concluding that occasional visits to United States were insufficient to invoke Fourth Amendment); United States v. Vatani, No. 06-20240, 2007 WL 789038, at *6 (E.D. Mich. Mar. 14, 2007) (holding that defendant lacked substantial connection to United States, despite "frequent[] travel" here).

As such, he does not have the right to invoke the Fourth Amendment to seek suppression of the Dutch Calls, which U.S. and Dutch authorities obtained through searches of the servers in the Netherlands. See United States v. Van Sichem, No. SS 89 CR. 813 (KMW), 1990 WL 144210, at *1 (S.D.N.Y. Sept. 26, 1990) ("Thus, because [the defendant] is a Dutch citizen who was residing in the Netherlands at the time of the search, even if he could demonstrate that Dutch officials were acting in concert with the United States government, he would not have any remedy."). Nor does he have the right to invoke the Fourth Amendment to seek suppression of the FlexiSpy Data, which the government obtained through the execution of search warrants in the United States. See, e.g., Gutierrez-Casada, 553 F. Supp. 2d at 1265.

"Under these circumstances, the Fourth Amendment has no application." Verdugo-Urquidez, 494 U.S. at 275; see United States v. Vega, No. 7-CR-707 (ARR), 2012 WL 1925876, at *5 (E.D.N.Y. May 24, 2012) (holding that defendant could not invoke Fourth Amendment, where "his only recent attachment to the United States involved the extraordinary international reach of his credit card fraud"); United States v. Gomez Castrillon, No. S2 05 CR. 156 (CM), 2007 WL 2398810, at *3 (S.D.N.Y. Aug. 15, 2007) (holding that defendants could not invoke Fourth Amendment to challenge interception of their telephone lines in Colombia, where they had "no voluntary attachment to the United States (other than their participation in various schemes to send controlled substances here)"). For this reason alone, the Court should deny the defendant's motions to suppress in their entirety.

B. The Defendant Has Failed to Meet His Burden to Establish Standing

Even if the defendant could invoke the Fourth Amendment (which he cannot), he has failed to meet his burden to prove standing to suppress the Dutch Calls and the FlexiSpy Data. "As the proponent of a motion to suppress, a defendant bears the burden of establishing

that he has 'standing' to challenge the search or seizure." United States v. Ashburn, 76 F. Supp. 3d 401, 411 (E.D.N.Y. 2014) (citing Rakas v. Illinois, 439 U.S. 128, 130 n.1. (1978)). "[T]he law is clear that the burden on the defendant to establish standing is met only by sworn evidence, in the form of affidavit or testimony, from the defendant or someone with personal knowledge." United States v. Rodriguez, No. 08 CR 1311 (RPP), 2009 WL 2569116, at *4 (S.D.N.Y. Aug. 20, 2009). "The defendant's unsworn assertion of the Government's representations does not meet this burden." Id.; see United States v. Montoya-Eschevarria, 892 F. Supp. 104, 106 (S.D.N.Y. 1995). Here, the defendant has not met his burden.

Even if the Court concluded, despite the contrary holding in Verdugo-Urquidez, that the defendant's trafficking of massive quantities of drugs to this country could establish the necessary connection to the United States for him to invoke the Fourth Amendment, his motion still must fail. The defendant has relied solely on the government's allegations that he was a drug trafficker to attempt to establish standing under the Fourth Amendment. See Dkt. No. 264 at 9-10. Under the law, this is insufficient. See Rodriguez, 2009 WL 2569116, at *4. If the defendant seeks to invoke the Fourth Amendment based on his drug trafficking to the United States, he must swear to those facts under penalty of perjury or submit other evidence. In the absence of such evidence, though, he lacks standing under the Fourth Amendment, and the Court must deny his motion. See id.

III. The Court Should Deny the Defendant's Motion to Suppress the Dutch Calls

The defendant argues that the Court should suppress the Dutch Calls under the Fourth Amendment. See Dkt. No. 263. In particular, he asserts that U.S. and Dutch authorities violated the Fourth Amendment by conducting the searches of the servers in the Netherlands that yielded the Dutch Calls. See id. at 7-11. The Court should reject this claim.

For the reasons discussed above, see section II supra, the defendant does not have standing to make this motion under Verdugo-Urquidez. But even assuming that he did, though, his arguments lack merit. When the defendant's severely diminished privacy interest in the Dutch Calls is weighed against the government's substantial interest in the searches for those calls, the searches were reasonable under the Fourth Amendment. Specifically, the defendant has failed to submit the necessary evidence to demonstrate his subjective expectation of privacy in the Dutch Calls; and, even if he had, he could not establish that his subjective expectation of privacy was objectively reasonable, in light of his status as an escapee and his workers' access to the Dutch Calls at the time of the searches at issue. Thus, he did not have a legitimate expectation of privacy in the Dutch Calls. Assuming that the defendant could establish such a privacy interest, though, the government's substantial interest in conducting the searches for those calls far outweighed it. The searches therefore were reasonable under the Fourth Amendment. Alternatively, the searches complied with the Fourth Amendment because the government conducted them pursuant to the CS's consent. Regardless, though, even if the Court concluded that the searches violated the Fourth Amendment, suppression still would not be warranted. Under the good-faith doctrine, U.S. authorities conducted the searches in objectively reasonable reliance on binding appellate precedent. The Court thus should deny the defendant's motion with respect to the Dutch Calls.

A. Legal Standard

"The Fourth Amendment protects the right of private citizens to be free from unreasonable government intrusions into areas where they have a legitimate expectation of privacy." United States v. Barner, 666 F.3d 79, 82 (2d Cir. 2012) (internal quotation marks omitted). "To this end, the Fourth Amendment restrains the government from engaging in

unreasonable searches and seizures, hence, the touchstone in evaluating the permissibility of any search is reasonableness." Id. at 83 (citations and internal quotation marks omitted). The Court examines "the totality of the circumstances to determine whether a search is reasonable within the meaning of the Fourth Amendment." Samson v. California, 547 U.S. 843, 848 (2006) (internal quotation marks omitted). "Reasonableness is determined 'by assessing, on the one hand, the degree to which a search intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." Barner, 666 F.3d at 82 (alteration and internal quotation marks omitted). "Reasonableness generally requires a warrant and probable cause[,] but the law recognizes certain exceptions to this rule." Id. (citations and internal quotation marks omitted).

Two such exceptions are relevant here. First, when U.S. officials conduct a search of U.S. citizens abroad, they are not required to obtain a warrant; the search is governed by the Fourth Amendment's reasonableness standard. See In re Terrorist Bombings of U.S. Embassies in E. Africa, 552 F.3d 157, 168 (2d Cir. 2008) ("In re Terrorist Bombings"). Second, "'[o]ne of the specifically established exceptions to the requirements of both a warrant and probable cause is a search that is conducted pursuant to consent.'" In re Terrorist Bombings, 552 F.3d at 168 (quoting Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973)).

Moreover, even where a court concludes that law enforcement officials have violated the Fourth Amendment, suppression does not necessarily follow. Under the good-faith doctrine, if law enforcement officers "act with an objectively reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence, the deterrence rationale loses much of its force, and exclusion cannot pay its way." Davis v. United States, 564 U.S. 229, 238 (2011) (citations and internal quotation marks

omitted). Suppression therefore is not warranted if officers conducted the search at issue in "strict compliance with then-binding Circuit law." Id. at 239.

B. The Defendant Has Failed to Meet His Burden to Establish a Legitimate Expectation of Privacy in the Dutch Calls

"A defendant seeking to suppress the fruits of a search by reason of a violation of the Fourth Amendment must show that he had a 'legitimate expectation of privacy' in the place searched." United States v. Nordlicht, No. 16-CR-00640 (BMC), 2018 WL 705548, at *3 (E.D.N.Y. Feb. 2, 2018) (internal quotation marks omitted). "This inquiry involves two distinct questions: first, whether the individual had a subjective expectation of privacy; and second, whether that expectation of privacy is one that society accepts as reasonable." Id. (internal quotation marks omitted). The burden is on the defendant to meet this standard. See id. Here, the defendant has established neither a subjective nor an objectively reasonable expectation of privacy. The Court therefore should deny his motion as to the Dutch Calls.

i. The Defendant Has Failed to Establish a Subjective Expectation of Privacy

"[I]t is well established that in order to challenge a search, a defendant must submit an affidavit from someone with personal knowledge demonstrating sufficient facts to show that he had a legally cognizable privacy interest in the searched premises at the time of the search." Nordlicht, 2018 WL 705548, at *3 (internal quotation marks omitted). As noted above, see section II.B. supra, "[t]he defendant's unsworn assertion of the Government's representations does not meet this burden." Rodriguez, 2009 WL 2569116, at *4.

Thus, to establish a subjective expectation of privacy in the Dutch Calls, the defendant must submit a sworn affidavit or testimony establishing his privacy interest in those communications. It is not sufficient to rely on government allegations, for instance, that the

government intercepted his communications or that he owned the servers in the Netherlands. See Dkt. No. 263 (citing government allegations in effort to establish reasonable expectation of privacy). The defendant must so swear in an affidavit or submit other evidence establishing those facts. See Rodriguez, 2009 WL 2569116, at *4 (concluding that defendant lacked standing to challenge intercepted communications, because he did not submit affidavit "establishing that it was the defendant's voice that was captured on the wiretap"); Montoya-Eschevarria, 892 F. Supp. at 106 (same). Because the defendant has failed to submit any sworn evidence in support of his motion, and instead has relied solely on government allegations, he has failed to meet his burden to establish a subjective expectation of privacy.

ii. The Defendant Has Failed to Establish an Objectively Reasonable Expectation of Privacy

Even assuming that the defendant has met his burden to establish a subjective expectation of privacy in the Dutch Calls, such an expectation of privacy would not be objectively reasonable. As an escapee from prison, the defendant had little or no expectation of privacy in those calls. Additionally, the defendant permitted the CS and his other workers to access the servers in the Netherlands as part of their duties for him; such access further diminished the defendant's expectation of privacy in the calls. Thus, the defendant had no expectation of privacy in the Dutch Calls that society would recognize as reasonable.

a. The Defendant's Status as an Escapee Severely Diminished His Expectation of Privacy

In United States v. Roy, 734 F.2d 108 (2d Cir. 1984), the Second Circuit held that, in light of his status as an escapee, the defendant lacked the legitimate expectation of privacy necessary to challenge the search of his automobile, id. at 111. The court stated that, "[a]t the time of the search and seizure, [the defendant] was no more than a trespasser on

society." Id. While his escape did not "deprive[] him of all expectations of privacy," the court considered "an escapee to be in constructive custody for the purpose of determining his legitimate expectations of privacy; he should have the same privacy expectations in property in his possession inside and outside the prison." Id. Reasoning that the defendant would not have had a reasonable expectation of privacy in an automobile on prison grounds, the court held that it "should not recognize such an expectation of privacy after he escapes." Id. So expanding his expectation of privacy following his escape "would offer judicial encouragement to the act of escape and would reward an escapee for his illegal conduct." Roy, 734 F.2d at 112; accord United States v. Edelman, 726 F.3d 305, 310 (2d Cir. 2013).

Moreover, "[a]fter the escape, the prison walls no longer protected the public from [the defendant]," and the "public's need for protection from [the defendant] argue[d] against according him any gr[e]ater Fourth Amendment rights because of his criminal act of escape." Roy, 734 F.2d at 112; see United States v. Ward, 561 F.3d 414, 418 (5th Cir. 2009) ("Allowing an escapee to invoke the privacy right would be inconsistent with protecting society from a demonstrably dangerous person who is fleeing from law enforcement outside of the structured environment that the criminal justice system determined was necessary for him."). The court therefore held, "[l]acking a legitimate expectation of privacy under the circumstances, [the defendant] cannot assert the unreasonableness of the search and seizure under the Fourth Amendment." Roy, 734 F.2d at 112; see also United States v. Cartwright No. 10-CR-104-CVE, 2010 WL 3931102, at *7 (N.D. Okla. Oct. 5, 2010) (collecting cases and stating that "[t]he finding that escaped prisoners have no reasonable expectation of privacy has been echoed by other courts and scholars"); cf. Samson v. California, 547 U.S. 843, 852 (2006) (stating that parolees "have severely diminished expectations of privacy by virtue of

their status alone"); United States v. Lambus, No. 16-4296, 2018 WL 3553324, at *38 (2d Cir. July 25, 2018) (concluding that parolee had "no reasonable or legitimate expectation of privacy that was violated by [GPS] monitoring").

Like the defendant in Roy, the defendant here was a "trespasser on society" at the time of the challenged searches in 2011. Roy, 734 F.2d at 111. Following the defendant's escape from prison in Mexico in 2001, he remained a fugitive until 2014. See Order Denying Def. Mot. to Dismiss, Oct. 6, 2017 Dkt. Entry ("The Government has more than sufficiently met its burden to show by a preponderance of the evidence that defendant was a fugitive fleeing from prosecution in both Mexico and the United States from 2001 until 2014, after he escaped from Mexican custody."). By 2011, the defendant was one of the most wanted men in the world, the U.S. and Mexican governments had offered substantial awards for his arrest and they were engaged in an intense manhunt for him. See Gov't Opp. to Def. Mot. to Dismiss, Dkt. No. 146 at 2-3; Gov't Mot. In Limine, Dkt. No. 213 at 28-31. Given his status as an escapee, the defendant did not have a legitimate expectation of privacy in his communications, including the Dutch Calls, as he would not have had an expectation of privacy in his communications in jail. See Tancredi v. Malfitano, 567 F. Supp. 2d 506, 511-12 (S.D.N.Y. 2008) (noting that "courts have generally refused to acknowledge a reasonable expectation of privacy for conversations which take place in prisons"). Such a conclusion is further warranted in light of the threat that the defendant posed to the public, not only from his massive drug trafficking to the United States, but also from the unprecedented acts of violence that he committed as the leader of the Sinaloa Cartel. See Roy, 734 F.2d at 112. The Court thus should conclude that the defendant had little, if any, expectation of privacy in the Dutch Calls. See Edelman, 726 F.3d at 310 (holding that escapee "did not have an objectively reasonable

expectation of privacy" in apartment); Ward, 561 F.3d at 417 (holding that escapee had no "constitutionally protected reasonable expectation of privacy" in motel room); United States v. Lucas, 499 F.3d 769 (8th Cir. 2007) ("As an escapee [the defendant] had only a minimal expectation of privacy in Scaife's apartment."); Gutierrez-Casada, 553 F. Supp. 2d at 1268 (noting that cases have extended Roy's "rationale to find that escaped prisoners in hotels or residences lack a legitimate expectation of privacy").

b. The Defendant's Workers' Access to the Dutch Servers Further Diminished His Expectation of Privacy

"It is well settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information." United States v. Jacobsen, 466 U.S. 109, 117 (1984). "Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information . . . ." Id. In accordance with these principles, the Supreme Court has held that "[w]hat [employees] observe in their daily functions is undoubtedly beyond the employer's reasonable expectation of privacy." Marshall v. Barlow's, Inc., 436 U.S. 307, 315 (1978); accord United States v. Longo, 70 F. Supp. 2d 225, 256 (W.D.N.Y. 1999) (adopting report and recommendation); see also Nordlicht, 2018 WL 705548, at *4 (evaluating third-party access to employee's computer and email in considering whether employee had reasonable expectation of privacy).

In this case, the defendant lacked any reasonable expectation of privacy in the servers. He did not set up and maintain the servers in the Netherlands on his own; rather, he hired workers to do so. The CS set up the servers in the Netherlands at the defendant's request

in 2011, and s/he was among the workers that the defendant tasked with maintaining that server throughout 2011. Thus, as part of his/her duties for the defendant, the CS and other workers had access to the Dutch Calls routed through the servers. Under these circumstances, the defendant had no expectation of privacy in the Dutch Calls at the time of the searches at issue in 2011. See United States v. Dupree, No. 10-CR-627 S-2 KAM, 2012 WL 5333946, at *31 (E.D.N.Y. Oct. 26, 2012), aff'd, 620 F. Appx. 49 (2d Cir. 2015) (concluding that suppression of emails was not warranted because defendant "did not have a legitimate expectation of privacy in emails that he gave [his employee] permission to access and view"); United States v. Segal, 299 F. Supp. 2d 856, 863 (N.D. Ill. 2004) ("Defendants' expectation that [employee] would not provide any documents to the Government was not reasonable."); Longo, 70 F. Supp. at 257 ("Accordingly, as to any viewing of computer files conducted by Schweter resulting from her status as Defendant's legal secretary, Defendant had no reasonable expectation of privacy in the directory and file names stored on the computer.").

To the extent that the defendant argues that his employee's status as a CS makes a difference in the analysis, this argument is contradicted by case law. See Dupree, 2012 WL 5333946, at *31 (assuming employee acted as government agent in rejecting suppression motion); Segal, 299 F. Supp. 2d at 863 (concluding defendants lacked reasonable expectation of privacy in documents that employee provided to government at its request, where employee had access to records as part of job duties). The Fourth Amendment does not "protect[] a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it." Hoffa v. United States, 385 U.S. 293, 302 (1966). Thus, the defendant's workers' access to the Dutch Calls further diminished whatever expectation of privacy, if any, he had in light of his status as an escapee.

For the reasons set forth above, the defendant has established neither a subjective nor an objectively reasonable expectation of privacy in the Dutch Calls. Thus, regardless of the government's interest in the search, the searches for those calls did not violate the Fourth Amendment. See Leventhal v. Knapek, 266 F.3d 64, 73 (2d Cir. 2001); Nordlicht, 2018 WL 705548, at *3. The Court should deny the defendant's motion as to the Dutch Calls.

C. The Government's Interest in the Search Outweighed the Defendant's Limited Privacy Interest

Insofar as the Court concludes that the defendant has established a legitimate expectation of privacy in the Dutch Calls, the Court nonetheless should conclude that the searches for those calls were reasonable under the Fourth Amendment. See In re Terrorist Bombings, 552 F.3d at 171. There is no dispute that U.S. and Dutch authorities searched servers in the Netherlands to obtain the Dutch Calls. The Fourth Amendment's warrant requirement thus does not apply to those searches; instead, the searches are constitutional if they were reasonable. See id. To make that determination, this Court must weigh the defendant's privacy interest in the Dutch Calls against the government's significant interest in conducting the searches at issue. See id. at 172. When the Court balances those competing interests, the government's interest far outweighs that of the defendant. The Court should thus conclude that the searches were reasonable.[15]

[15] The standard set forth in In re Terrorist Bombings applies to U.S. authorities' searches of U.S. citizens abroad. 552 F.3d at 167. As discussed above, see section II supra, under Verdugo-Urquidez, the Fourth Amendment does not apply to the defendant, who was a foreign citizen living abroad. The government has assumed arguendo that the standard in In re Terrorist Bombings applies to the defendant here.

In this regard, the Second Circuit decision in In re Terrorist Bombings is instructive. There, the defendant, a citizen of the United States, challenged the U.S. government's electronic surveillance of him abroad. In affirming the district court's denial of his suppression motion, the Second Circuit recognized that the defendant had a significant expectation of privacy in his telephonic communications.[16] Nevertheless, despite the "significant invasion of privacy" occasioned by the government's surveillance in that case, the court upheld the search as reasonable under the Fourth Amendment. Id. at 175-76.

In so holding, the court cited four factors that justified the search. See id. "First, complex, wide-ranging, and decentralized organizations, such as al Qaeda, warrant sustained and intense monitoring in order to understand their features and identify their members." Id. at 176. Second, "foreign intelligence gathering of the sort considered here must delve into the superficially mundane because it is not always readily apparent what information is relevant." Id. Third, "members of covert terrorist organizations, as with other sophisticated criminal enterprises, often communicate in code, or at least through ambiguous language." Id. "Hence, more extensive and careful monitoring of these communications may be necessary." Id. Finally, "because the monitored conversations were conducted in foreign languages, the task of determining relevance and identifying coded language was further complicated." Id. Based on these four factors, the court ruled that, "while the intrusion on [the defendant's] privacy was great, the need for the government to so intrude was even greater." Id.

[16] Unlike the defendant here, see section III.B.ii. supra, the defendant in that case did not have a diminished expectation of privacy due to his status as an escapee and third-party access to his communications. See In re Terrorist Bombings, 552 F.3d at 175.

Here, while the defendant's privacy interest in the Dutch Calls is far less weighty than the privacy interest identified in In re Terrorist Bombings, see section III.B. supra, the government's interest in the search is just as compelling. All four factors that the Second Circuit cited in its opinion apply with equal force here:

- First, the Sinaloa Cartel is a "complex, wide-ranging, and decentralized organization." 552 F.3d at 175. In fact, at the time of the search, the Sinaloa Cartel was the largest and most violent drug trafficking organization in the world, with thousands of members scattered throughout the world, primarily in North, South and Central America. The government necessarily needed to engage in "sustained and intense monitoring in order to understand [its] features and identify [its] members." Id. For example, the government captured many Cartel members' voices in the calls; without sustained and intense monitoring, the government could not have identified them, their locations and their respective roles in the Cartel.

- Second, and relatedly, to identify the members of the Cartel and to attempt to pin down their locations, the government had to "delve into the superficially mundane." Id. A key piece of identifying information, such as the name of a caller or a family member or a critical reference to the location of a Cartel member, often came interspersed in relatively mundane communications. Furthermore, the calls taken together painted a picture of how the Cartel operated in a way that individual calls could not. See id. at 176 (noting that "innocent-sounding conversations may later prove to be highly significant" and "individual items of information, not apparently significant when taken in isolation, may become highly significant when considered together over time" (internal quotation marks omitted)).

- Third, Sinaloa Cartel members often spoke in code and ambiguous language during the Dutch Calls, which required the government to monitor carefully the communications to decipher the calls over time. See id. (citing United States v. Casamento, 887 F.2d 1141, 1190 (2d Cir. 1989) (recognizing that conspirators in a complex narcotics scheme spoke in code)).

- Finally, the Sinaloa Cartel members invariably spoke in Spanish during the Dutch Calls. The FBI thus had translators translate the calls, so that English-speaking agents could review them for relevance and code. This process further complicated the monitoring. See id.

Accordingly, pursuant to In re Terrorist Bombings, the government's interest in conducting the searches that yielded the Dutch Calls far outweighed the defendant's minimal

or non-existent privacy interest in those calls. While monitoring the Dutch Calls, the government actively sought to gather information to capture the defendant and his coconspirators, disrupt their drug trafficking and acts of violence and map their far-reaching criminal network. The absence of the Dutch Calls during 2011 would have significantly impeded the government's efforts to do so. The government thus had a paramount interest in obtaining those calls. It therefore obtained the Dutch Calls through MLAT requests for judicially authorized electronic surveillance and search warrants when such methods were available. See id. at 173-74 (considering foreign warrant as one factor that weighed in favor of finding search of foreign home reasonable). If the government was not able to obtain the calls through MLAT requests, due to technical difficulties in the Dutch interception method or delay in obtaining the judicial interception orders, the FBI agents directed the CS to obtain the calls directly from the servers in the Netherlands. The CS then provided them to the FBI via email. Had the FBI not directed the CS to obtain those calls, the calls likely would have been lost entirely. Given the overwhelming government interest in obtaining the Dutch Calls, including the need to attempt to thwart the defendant's drug trafficking and violent crimes, the government acted reasonably both in obtaining them directly through the CS, as well as through the MLAT process. The searches did not violate the Fourth Amendment.[17]

[17] The defendant argues that Dutch authorities acted as agents of U.S. authorities in conducting the searches that yielded the Dutch Calls. See Dkt. No. 264 at 7-9. As discussed above, the government directly obtained certain Dutch Calls from the servers in the Netherlands, when the CS retrieved calls from those servers and emailed them to FBI agents. It obtained the remaining Dutch Calls through MLAT requests to the Netherlands for judicially authorized electronic surveillance and search warrants of the servers in the Netherlands. As to the latter category, except in limited circumstances, the requirements of the Fourth Amendment do not apply to foreign officials conducting searches abroad. See Defreitas, 701 F. Supp. 2d at 305. Such limited circumstances include "(1) where the conduct of foreign law enforcement officials rendered them agents, or virtual agents, of United States law

D. The CS Consented to the Search for the Dutch Calls

Alternatively, the searches that yielded the Dutch Calls did not violate the Fourth Amendment, because the CS consented to them. "Consent may be given by a third party who possess[es] common authority over or other sufficient relationship to the premises or effects sought to be inspected." United States v. Yudong Zhu, 23 F. Supp. 3d 234, 238 (S.D.N.Y. 2014) (alteration in original; internal quotation marks omitted). In United States v. Davis, 967 F.2d 84 (2d Cir. 1992) ("Davis II"), the Second Circuit articulated a two-part test concerning third-party consent: such consent is valid if "first, the third party had access to the area searched, and, second, either: (a) common authority over the area; or (b) a substantial interest in the area; or (c) permission to gain access," id. at 87. "[C]ommon authority is, of course, not to be implied from the mere property interest a third party has in the property. [It] rests rather on mutual use of the property by persons generally having joint access or control for most purposes . . . ." Yudong Zhu, 23 F. Supp. 3d at 238 (second alteration and ellipsis in original; internal quotation marks omitted).

Here, the CS indisputably had access to the Dutch Calls on the servers in the Netherlands. Additionally, as part of his/her employment with the defendant—who had paid the CS to set up and maintain the servers in the Netherlands at the time of the searches in

---

enforcement officials; or (2) where the cooperation between the United States and foreign law enforcement agencies is designed to evade constitutional requirements applicable to American officials." Id. The government disputes that these narrow exceptions are present here. See, e.g., United States v. Getto, 729 F.3d 221, 230-33 (2d Cir. 2013) ("It is not enough that the foreign government undertook its investigation pursuant to an American MLAT request."). The Court, however, need not decide whether they apply in this case. For the reasons stated above, even if U.S. authorities directed the searches by the Dutch authorities, the searches were reasonable under the Fourth Amendment. See Defreitas, 701 F. Supp. 2d at 305.

2011—the CS had common authority over the servers, a substantial interest in them and permission to gain access. The CS thus had the right to consent to the FBI search of the servers, and he did so when he provided FBI agents and Dutch authorities access to the calls on them. See United States v. Marandola, 489 Fed. Appx. 522, 523 (2d Cir. 2013) (holding that wife had authority to consent to search of husband's computer where, among other things, she had access to computer and used it sparingly); Yudong Zhu, 23 F. Supp. 3d at 238 (concluding that employer, which had authorization to access employee's computer, had authority to consent to search of computer); see also United States v. Lang, 717 Fed. Appx. 523, 542 (6th Cir. 2017) (concluding that employee properly could consent to search of employer's exam room).

The CS's status as an informant did not vitiate his authority to consent to the search. Courts of Appeals to confront this question have uniformly concluded that an informant may validly consent to a search of a defendant's property, if he has actual or apparent authority over that property. See Lang 717 Fed. Appx. at 543 (citing United States v. Apperson, 441 F.3d 1162, 1186-87 (10th Cir. 2006)); Wang v. United States, 947 F.2d 1400, 1403 (9th Cir. 1991)). "The Fourth Amendment . . . does not protect wrongdoers from misplaced confidence in their associates." Id. at 542 (ellipsis in original; internal quotation marks omitted). Thus, courts have "rejected complaints that a defendant never consented to the presence of a 'police spy' in his home." Id. (internal quotation marks omitted). Here, the CS could consent to the FBI and Dutch authorities' searches of the servers by virtue of the CS's authority over those servers as part of his/her work for the defendant. The defendant may not complain that the CS "used that authority to let [the FBI] enter." Id.; see Jacobsen, 466 U.S. at 117. Accordingly, because the CS consented to the searches that yielded the Dutch Calls, those searches did not violate the Fourth Amendment.

E. The FBI Agents Acted in Good Faith in Conducting the Searches for the Dutch Calls

Even if the Court concludes that the FBI agents violated the Fourth Amendment in obtaining the Dutch Calls, the Court still should not suppress that evidence. Under Davis, the FBI agents acted in good-faith reliance on binding appellate precedent. The Court should thus deny the defendant's motion under the good-faith doctrine.

i. The Good-Faith Doctrine under *Davis*

In Davis, the Supreme Court stated that the exclusionary rule is a "prudential doctrine created . . . to compel respect for constitutional guaranty." 564 U.S. at 236 (citations and internal quotation marks omitted). "Exclusion is not a personal constitutional right, nor is it designed to redress the injury occasioned by an unconstitutional search." Id. (internal quotation marks omitted). The Supreme Court thus has "limited the rule's operation to situations in which this purpose is thought most efficaciously served." Id. at 237 (internal quotation marks omitted). "Where suppression fails to yield appreciable deterrence, exclusion is clearly unwarranted." Id. (alteration and internal quotation marks omitted).

"Real deterrent value is a necessary condition for exclusion, but it is not a sufficient one." Id. (internal quotation marks omitted). "The analysis must also account for the substantial social costs generated by the rule." Id. (internal quotation marks omitted). Indeed, the Court stated in Davis:

> Exclusion exacts a heavy toll on both the judicial system and society at large. It almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence. And its bottom-line effect, in many cases is to suppress the truth and set the criminal loose in the community without punishment. Our cases hold that society must swallow this bitter pill when necessary, but only as a last resort. For exclusion to be

> appropriate, the deterrence benefits of suppression must outweigh its heavy costs.

Id. (citations and internal quotation marks omitted). Thus, "when the police act with an objectively reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence, the deterrence rationale loses much of its force, and exclusion cannot pay its way." Id. at 238 (citations and internal quotations marks omitted).

Applying these principles, Davis held that the Fourth Amendment violation at issue in that case did not warrant application of the exclusionary rule, because the search was conducted in "strict compliance with then-binding Circuit law and was not culpable in any way." Id. at 239-40. It concluded that, "[a]bout all that exclusion would deter in this case is conscientious police work." Id. at 241. "[W]hen binding appellate precedent specifically authorizes a particular police practice, well-trained officers will and should use that tool to fulfill their crime-detection and public-safety responsibilities." Id. (emphasis in original). Therefore, "[a]n officer who conducts a search in reliance on binding appellate precedent does no more than act as a reasonable officer would and should act under the circumstances." Id. (alteration and internal quotation marks omitted). "The deterrent effect of exclusion in such a case can only be to discourage the officer from doing his duty." Id. (alteration and internal quotation marks omitted). As this is not the "kind of deterrence the exclusionary rule seeks to foster," the Court held that "[e]vidence obtained during a search conducted in reasonable reliance on binding precedent is not subject to the exclusionary rule." Id.

ii. The FBI Agents Acted in Good Faith

In this case, the FBI agents acted in objectively reasonable reliance on the foregoing appellate precedent, see sections II & III supra, in conducting the searches that

yielded the Dutch Calls. In particular, at the time of the searches at issue in 2011, (1) Verdugo-Urquidez had established that the Fourth Amendment did not apply to searches of foreign citizens conducted abroad, see section II supra; (2) Roy had established that escapees had a severely diminished expectation of privacy, see section III.B.ii.a. supra; (3) Marshall had established that an employer lacked a reasonable expectation of privacy in what his employees observed as party of their duties, see section III.B.ii.b. supra; (4) In re Terrorist Bombings had established that the warrant requirement does not apply to searches abroad and that the government has a compelling interest in disrupting complex criminal organizations, see section III.B.ii.b. supra; and (5) Davis II had articulated the two-part test to evaluate a third-party's consent to an area over which he has common authority with the defendant, see section III.E. supra. Under this precedent, it was objectively reasonable for the FBI agents to believe that they and the Dutch authorities did not violate the Fourth Amendment by conducting the searches that yielded the Dutch Calls. As such, applying the exclusionary rule in this case would serve no deterrent purpose.

IV. The Court Should Deny the Defendant's Motion to Suppress to the FlexiSpy Data

The defendant argues that this Court should suppress the FlexiSpy Data. See Dkt. No. 263. Specifically, he claims that (1) the government unlawfully seized certain FlexiSpy Data prior to the execution of FlexiSpy Warrants I & II; (2) FlexiSpy Warrant III lacked particularity; (3) FlexiSpy Warrant III violated Federal Rule of Criminal Procedure 41; and (4) the foregoing constitutional violations tainted FlexiSpy Warrants IV-XV.

For the reasons discussed above, see section II supra, Verdugo-Urquidez forecloses this motion. In any event, though, the defendant's arguments are meritless. The government lawfully copied the FlexiSpy Data prior to the execution of FlexiSpy Warrants I

& II, and FlexiSpy Warrant III complied with the Fourth Amendment. Regardless, even assuming a Fourth Amendment violation, the good-faith doctrine applies. Moreover, under the corrected-affidavit doctrine, any constitutional violation in FlexiSpy Warrants I-III would not taint FlexiSpy Warrants IV-XV. The Court thus should deny the defendant's motion with respect to the FlexiSpy Data.

A. The Copying of the FlexiSpy Data Prior to the Execution of FlexiSpy Warrants I & II Did Not Violate the Fourth Amendment

The defendant claims that the government unlawfully seized the FlexiSpy Data prior to the execution of FlexiSpy Warrants I & II. See Dkt. No. 263 at 8-10. Not so. The copying of the FlexiSpy Data prior to the execution of FlexiSpy Warrants I & II did not constitute a "seizure" under the Fourth Amendment and, even if it did, such a seizure was reasonable. But even if such action did violate the Fourth Amendment, the independent source doctrine applies, and suppression is not appropriate. The Court thus should deny the defendant's motion as it pertains to FlexiSpy Warrants I & II.

i. The Government Did Not Seize the FlexiSpy Data Prior to Executing FlexiSpy Warrants I & II

"[A] seizure of property occurs for purposes of the Fourth Amendment if the police meaningfully interfere with an individual's possessory interest in that property." United States v. Robertson, 239 F.Supp.3d 426, 442 (D. Conn. 2017) (citing Soldal v. Cook Cty., 506 U.S. 56, 61 (1992)). The "act of recording visible information," for instance, by photographing or photocopying that information, does not constitute a seizure under the Fourth Amendment. United States v. Simmons, No. 13-CR-6025CJS, 2016 WL 285176, at *21 (W.D.N.Y. Jan. 22, 2016), report and recommendation adopted, No. 13-CR-6025, 2016 WL 1127802 (W.D.N.Y. Mar. 23, 2016) (collecting cases); see Arizona v. Hicks, 480 U.S. 321, 324 (1987) (holding

that "mere recording of the serial numbers did not constitute a seizure" because it did not "meaningfully interfere with respondent's possessory interest" (internal quotation marks omitted)).

Courts have applied these principles to the copying of electronic data. See, e.g., In re Search of Info. Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc., No. 16-MJ-00757 (BAH), 2017 WL 3445634, at *16 (D.D.C. July 31, 2017) ("In re Gmail Search") ("The mere transfer by Google of customer information from a server in a foreign country to Google's data center in California does not amount to a search or a seizure." (internal quotation marks omitted)); In re Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708, 720 (E.D. Pa. 2017) ("In re Google Warrant I") ("Electronically transferring data from a server in a foreign country to Google's data center in California does not amount to a 'seizure' because there is no meaningful interference with the account holder's possessory interest in the user data."), aff'd, 275 F. Supp. 3d 605 (E.D. Pa. 2017) ("In re Google Warrant II"); Gorshkov, 2001 WL 1024026, at *3 ("[T]he agents' act of copying the data on the Russian computers was not a seizure under the Fourth Amendment because it did not interfere with Defendant's or anyone else's possessory interest in the data."). The copying of electronic data is akin to taking a snapshot of that data. See In re Google Warrant I, 232 F. Supp. 3d at 720. Such action does not meaningfully interfere with the possessory rights of the owner of the data, because the owner of the data continues to be able to access the data despite the copying of it. See Gorshkov, 2001 WL 1024026, at *3 (noting that, despite agents' copying of data, it "remained intact and unaltered" and "accessible to Defendant and any

co-conspirators or partners with whom he had shared access").[18] Hence, the copying of data does not constitute a seizure under the Fourth Amendment. See id.

Here, prior to obtaining FlexiSpy Warrant I, at the direction of FBI agents, the CS "logged into the FlexiSpy website, accessed the spyware accounts using the usernames and passwords (which he had retained after purchasing the licenses), and downloaded all of the text messages, Blackberry messages, call logs/toll records, GPS location data, and other data onto an Amazon server owned by the FBI." Ex. S at 12147A-12148A.[19] "FBI agents then downloaded the files onto [a] DVD," for which it later obtained the search warrant. Id. at 12148A. In copying that data, the FBI agents did not interfere with the defendant's possessory interest. On the contrary, the FBI agents intended for neither the defendant nor his coconspirators who accessed the data on a regular basis to be aware that the FBI agents had access to the data. Had the FBI agents deprived the defendant and his coconspirators of access to the data it would have risked alerting them to the fact that the FBI agents also had access to the data, and they likely would have stopped using the FlexiSpy software. Thus, depriving the defendant of access to the data would have thwarted the FBI's efforts to gather the FlexiSpy Data on an ongoing basis through serial search warrants. The FBI agents thus had no intention of—and, in fact, did not—deprive the defendant and his coconspirators of access to the

[18] Federal Rule of Criminal Procedure 41(e)(2)(B), which addresses warrants seeking electronically stored information, specifically distinguishes between "the seizure or on-site copying of the media or information." This distinction further illustrates that copying data does not constitute a seizure. That distinction is also apparent in Attachment A to FlexiSpy Warrant III, which authorizes copying of the FlexiSpy Data in the designated accounts. See Ex. U at 12214A.

[19] The government does not dispute that the CS acted at the direction of the FBI agents in downloading the FlexiSpy Data prior to the execution of FlexiSpy Warrants I & II. See Dkt. No. 263 (arguing that copying of FlexiSpy Data involved government action).

FlexiSpy Data. Therefore, "[t]he copying of the data had absolutely no impact on his possessory rights," and "it was not a seizure under the Fourth Amendment." Gorshkov, 2001 WL 1024026, at *3.

In an opinion recently vacated as moot by the Supreme Court, the Second Circuit held that Microsoft, acting as an agent of the government, "seized" data from its foreign data center when it copied that data and provided it to the government in response to a search warrant. See Microsoft Corp. v. United States, 829 F.3d 197, 220 (2d Cir. 2016) ("Microsoft"), vacated and remanded sub nom. United States v. Microsoft Corp., 138 S. Ct. 1186 (2018). This Court should decline to apply Microsoft's holding here for several reasons.

First, it is not binding precedent. "[B]y definition, vacating a decision divests that decision of legal force." Sajous v. Decker, No. 18-CV-2447 (AJN), 2018 WL 2357266, at *6 (S.D.N.Y. May 23, 2018). Rather, it carries only "persuasive authority." Id. (internal quotation marks omitted); see United States v. Gasperini, 894 F.3d 482, 488 (2d Cir. 2018) (assuming, without deciding, that "ruling in Microsoft—which was vacated as moot by the Supreme Court—correctly states the law").

Second, because half of the active judges on the Second Circuit have rejected Microsoft, it carries little persuasive force following the Supreme Court's vacatur. "Although the panel decision in the Microsoft case was unanimous, the decision drew vigorous opposition from other judges of the Second Circuit when the case came before the full court on the government's petition for rehearing en banc." In re Google Warrant II, 275 F. Supp. 3d at 612; see Microsoft Corp. v. United States, 855 F.3d 53 (2d Cir. 2017) ("Microsoft Reh'g") (denying rehearing en banc). "The petition was denied by an equally divided court, but the denial generated four separate dissents . . . ." In re Google Warrant II, 275 F. Supp. 3d at 612. In her

dissent joined by the three other dissenting judges, Judge Raggi "rejected the majority panel's ruling that Microsoft's accessing of the emails in Ireland constituted a seizure." In re Google Warrant I, 232 F. Supp. 3d at 721 n.15 (citing Microsoft Reh'g, 855 F.3d at 72 (Raggi, J., dissenting)). "Judge Raggi reasoned that 'it is simply wrong to characterize Microsoft's actions in retrieving customer electronic data in Ireland . . . as a seizure by Microsoft.'" Id. (quoting Microsoft Reh'g, 855 F.3d at 72).

Third, other courts' rejection of Microsoft further underscores its lack of persuasive force. Indeed, in the wake of Microsoft, other courts have roundly declined to follow its reasoning. See, e.g., In re Google Warrant II, 275 F. Supp. 3d at 613 ("The Microsoft court's analysis has also been rejected by every magistrate judge and district court that has considered the issue to date, including the Magistrate Judge in this case."). Many of those courts specifically declined to follow Microsoft's conclusion that copying data constituted a seizure of that data. See, e.g., In re Gmail Search, 2017 WL 3445634, at *16; In re Google Warrant I, 232 F. Supp. 3d at 719.

Finally, as discussed above, Microsoft conflicts with established Supreme Court precedent regarding the meaning of a "seizure" under the Fourth Amendment. See Soldal, 506 U.S. at 61; Jacobsen, 466 U.S. at 113. For a seizure of property to occur under that Amendment, the government must interfere with a person's possessory interests. See Jacobsen, 466 U.S. at 113. By holding that Microsoft seized data on behalf of the government without interfering with such interests, Microsoft is at odds with that Supreme Court precedent.

Accordingly, for the foregoing reasons, the Court should conclude that the government did not seize the FlexiSpy Data within the meaning of the Fourth Amendment

prior to executing FlexiSpy Warrants I & II. The Court thus should deny the defendant's motion with respect to those warrants.

ii. Assuming the Government Seized the FlexiSpy Data, Such Seizure was Reasonable

The defendant does not dispute that the government had probable cause to seize the FlexiSpy Data. See Dkt. No. 263 at 8-10. Nor could he reasonably do so, given the magistrate judges' determinations that probable cause existed based on the affidavits in support of FlexiSpy Warrants I & II. Rather, he contends that the government impermissibly seized the FlexiSpy Data without a warrant. See id. at 10. Assuming that the government seized the FlexiSpy Data, however, the government, properly did so without a warrant to avoid "loss or destruction of suspected contraband." United States v. Martin, 157 F.3d 46, 53 (2d Cir. 1998) (internal quotation marks omitted).

"'[W]here law enforcement authorities have probable cause to believe that a container holds contraband or evidence of a crime, but have not secured a warrant, the Supreme Court has interpreted the Fourth Amendment to permit seizure of the property, pending issuance of a warrant to examine its contents, if the exigencies of the circumstances demand it or some other recognized exception to the warrant requirement is present.'" United States v. Okparaeka, No. 17-CR-225 (NSR), 2018 WL 3323822, at *4 (S.D.N.Y. July 5, 2018) (alterations omitted) (quoting Martin, 157 F.3d at 53).

"Electronic data and evidence is notoriously ephemeral." Gorshkov, 2001 WL 1024026, at *3 n.2. "It can be moved to a different computer with each, or access to it can be prevented with a simple change of password or pull of the power plug." Id. At the time the CS downloaded the FlexiSpy Data, the government was aware that the defendant and his

coconspirators regularly accessed the FlexiSpy Data to monitor the defendant's girlfriends and others; thus, any delay in copying the data risked its loss or destruction. See Gorshkov, 2001 WL 1024026, at *3 ("The agents had good reason to fear that if they did not copy the data, Defendant's coconspirators would destroy the evidence, or make it unavailable before any assistance could be obtained . . ."). In fact, the defendant and/or his workers did delete FlexiSpy Data on the Amazon cloud server during the course of the FBI investigation.

In an effort to obtain the FlexiSpy Data, FBI agents had consulted with representatives of Cloudflare and Amazon as to whether those companies could retrieve the data in response to a search warrant. See, e.g., Ex. S at 12147A. As a result of those consultations, the FBI agents learned that Cloudflare did not possess the data and "that due to the nature of how cloud servers store the data, it would be extremely difficult, and potentially impossible, for Amazon to locate the requested data, even with the usernames and passwords for the accounts." Id. Thus, although Amazon had possession of the data, it could not provide it to the FBI in response to the search warrant. FBI agents therefore took steps to access and copy the data to preserve it while they obtained a warrant. Once downloaded, the agents did not examine the FlexiSpy Data prior to obtaining the warrants. The agents thus "made reasonable efforts to reconcile their needs with" any privacy interest the defendant may have had "by copying the data, without altering it or examining its contents until a search warrant could be obtained." Gorshkov, 2001 WL 1024026, at *4. Accordingly, "because the agents were acting under exigent circumstances, their actions in accessing the [FlexiSpy Data] and downloading the data without a warrant were fully legal and the evidence should not be suppressed." Id.

Insofar as the defendant claims that the government's 15-day delay in obtaining FlexiSpy Warrant I following the copying of the FlexiSpy Data on December 22, 2011 was unreasonable, see Dkt. No. 263 at 9-10, he is wrong. "Where, as here, a warrantless seizure is followed by a delay in securing a search warrant, Court's must conclude whether such delay is constitutionally unreasonable." Okparaeka, 2018 WL 3323822, at *5. "'In determining the reasonableness of the government's delay in seeking a search warrant after a valid seizure, a court looks to various factors, including the length of time for which the individual was deprived of her or his property, any diminished interest in the property that the individual may have had, and whether the seizure affected the individual's liberty interests, for example, where an officer seizes a traveler's luggage and thereby disrupts that individual's travel plans.'" United States v. Mathews, No. 18-CR-124 (JPO), 2018 WL 2277839, at *3 (S.D.N.Y. May 17, 2018) (quoting United States v. Howe, 545 Fed. Appx. 64, 65-66 (2d Cir. 2013)). "The court also analyzes the government's interests in seizing the property, and balances the competing interests." Id. (internal quotation marks omitted). Here, the record shows that the 15-day delay was reasonable.

First, "the delay included two weekends and the Christmas [and New Year] holiday[s], which could explain the difficulty in promptly obtaining the warrant." Martin, 157 F.3d at 54; see Mathews, 2018 WL 2277839, at *3 ("[A]s in Martin, the delay included two weekends and the Christmas holiday, which could explain the difficulty in promptly obtaining the warrant." (internal quotation marks omitted)); Okparaeka, 2018 WL 3323822, at *7 (concluding that delay was "especially short because it included three weekends as well as the Passover holiday"). Second, the defendant had little, if any, expectation of privacy in the intercepted communications in light of his status as an escapee and the access of his workers,

including the CS, to the FlexiSpy Data. See Section III.B.ii supra. Thus, he had a "diminished interest in the property." Mathews, 2018 WL 2277839, at *4. Lastly, the copying of the data interfered with neither the defendant's liberty interests nor his property interests; indeed, the defendant continued to live freely abroad in Mexico with full access to the data during those 15 days. Under these circumstances, the 15-day delay was reasonable. See Martin, 157 F.3d at 54 (11-day delay reasonable); Mathews, 2018 WL 2277839, at *3 (17-day delay reasonable); Okparaeka, 2018 WL 3323822, at *7 (19-day delay reasonable).[20]

iii. Suppression is Not Justified Under the Independent Source Doctrine

Even assuming that the FBI agents unlawfully seized the FlexiSpy Data, suppression still would not be justified under the independent source doctrine. As the Second Circuit has held, "the independent source doctrine requires that: (1) the warrant [was] supported by probable cause derived from sources independent of the illegal[ity]; and (2) the decision to seek the warrant [was not] prompted by information gleaned from the illegal conduct." United States v. Nayyar, 221 F. Supp. 3d 454, 466 (S.D.N.Y. 2016), aff'd sub nom. United States v. Mulholland, 702 F. Appx. 7 (2d Cir. 2017) (alterations in original). "Thus, under the independent source doctrine, objects that have been illegally seized may be

[20] The defendant asserts that the FBI agent lied in her affidavit in support of FlexiSpy Warrant I when she asserted that the government did not access the FlexiSpy Data until it obtained a warrant. See Dkt. No. 263 at 9. This accusation is completely baseless and is not grounds for suppression. See United States v. Scully, 108 F. Supp. 3d 59, 96 (E.D.N.Y. 2015) (stating that "conclusory" allegations of falsehoods unsupported by "offer of proof" and "statement of supporting reasons" are insufficient to justify hearing under Franks v. Delaware, 438 U.S. 154, 171 (1978)).

re-seized even if the illegal seizure came first in a sequence of events leading to the legal seizure." Id. at 467.

Here, "the evidence at issue is not subject to suppression because it was obtained through the independent source of a valid search warrant that did not depend upon anything observed during the copying and downloading of the files." Gorshkov, 2001 WL 1024026, at *5. "Probable cause for [FlexiSpy Warrants I & II] was based entirely upon information that was independent of the copying and downloading." Id. "As a result, the affidavit provided an independent source for the warrant." Id. (citing Segura v. United States, 486 U.S. 796, 799, 813-16 (1988) (plurality opinion) (affidavit provided independent source where there was abundant probable cause and agents in no way exploited their warrantless entry into apartment)); see Mulholland, 702 F. Appx. at *11 (affirming district court's application of independent source doctrine, noting that "search warrant application [for computer] did not rely on anything discovered during the initial warrantless search"). Because the independent source doctrine applies here, the Court should deny the defendant's suppression motion as to FlexiSpy Warrants I & II.

B. FlexiSpy Warrant III Neither Violated the Fourth Amendment Nor Rule 41

The defendant challenges FlexiSpy Warrant III on the ground that it was not sufficiently particular under the Fourth Amendment. See Dkt. No. 263 at 11-12. He further contends that the warrant violated Rule 41. See id. at 13-15. Because the warrant was sufficiently particular and fully complied with Rule 41, the Court should deny the defendant's motion as it pertains to FlexiSpy Warrant III.

i. FlexiSpy Warrant III Did Not Lack Particularity

The Fourth Amendment requires "particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. "The particularity requirement has three components." Nordlicht, 2018 WL 705548, at *6 (internal quotation marks omitted). "First, a warrant must identify the specific offense for which the police have established probable cause." Id. (internal quotation marks omitted). "Second, a warrant must describe the place to be searched." Id. (internal quotation marks omitted). "Third, the warrant must specify the items to be seized by their relation to designated crimes." Id. (internal quotation marks omitted). "However, the standard for constitutional particularity requires only that a warrant be sufficiently specific to permit the rational exercise of judgment by the executing officers in selecting what items to seize." Id. (internal quotation marks omitted).

"The nature of the crime, for example, may require a broad search." Id. (internal quotation marks omitted). Indeed, the requisite particularity decreases as the complexity of the crime involved increases. See United States v. Dupree, 781 F. Supp. 2d 115, 149 (E.D.N.Y. 2011); see also United States v. Cohan, 628 F. Supp. 2d 355, 362 (E.D.N.Y. 2009) (stating that "lengthy list of categories" permissible when investigating complex scheme); United States v. Gotti, 42 F. Supp. 2d 252, 274 (S.D.N.Y. 1999) (concluding that "generic terms" permissible when investigating complex scheme); United States v. Cioffi, 668 F. Supp. 2d 385, 391 (E.D.N.Y. 2009) (stating that documentary evidence may be described with less particularity than murder weapon or stolen property). The Second Circuit has held that narcotics crimes are among the crimes that permit greater generalization in the warrant. See, e.g., United States v. Washington, 48 F.3d 74, 77 (2d Cir. 1995) (deciding warrant to search "[a]ny and all papers, records, receipts, documentation, telephone lists and records which may be related to illicit

drug activities" was sufficiently particular); United States v. Riley, 906 F.2d 841, 843, 845 (2d Cir. 1990) (holding that categories of records "and other items that constitute evidence of" drug crimes sufficiently particular, with the court deeming latitude was warranted by "recogniz[ing] the reality that few people keep documents of their criminal transactions in a folder marked 'drug records'"); United States v. Young, 745 F.2d 733, 758 (2d Cir. 1984) (deeming warrant for narcotics and "notes, documents and papers and other evidence of" narcotics conspiracy sufficiently particular).

Here, FlexiSpy Warrant III was sufficiently particular.[21] First, in Attachment A, the government described the specific offenses for which the police had probable cause to search, namely, "trafficking of narcotics or laundering of drug proceeds." Ex. U at 12214A, 12264A. Moreover, in the warrant application and affidavit in support, the government listed specific statutes for which it had probable cause to search, namely, 21 U.S.C. §§ 959, 963. See Ex. U at 12216A, 12218A 12266A, 12268A. Second, the warrant specifically described the place to be searched, listing 35 specific FlexiSpy Accounts in the possession of Amazon for which the warrant authorized the search. See Ex. U at 12214A, 12264A. Third, it narrowed the information that could be copied to that which related to data that, "from the law enforcement personnel's review (with the assistance of an interpreter, if necessary), based on the content of the communications or data, appear to be pertinent to the trafficking of narcotics offenses or laundering of drug proceeds." Ex. U at 12214A, 12264A. Accordingly, FlexiSpy

[21] As previously noted, FlexiSpy Warrant III included both a warrant to search the FlexiSpy accounts and a warrant to collect GPS data related to the cellular telephones associated with those accounts. See Ex. U. Because the portions of the warrant pertinent to the defendant's motion are identical, the government discusses them together.

Warrant III comported with the Fourth Amendment's particularity requirement. See Nordlicht, 2018 WL 705548, at *6.

In urging a contrary conclusion, the defendant claims that the warrant is invalid because it did not list "the specific offenses" in the "FlexiSpy Search Warrant or in Attachment A." Dkt. No. 263 at 11. Presuming that the defendant is arguing that the warrant is deficient because the warrant form and Attachment A did not list the particular statutes at issue, there is no such requirement.[22] See Washington, 48 F.3d at 77 (concluding warrant to search for evidence "related to illicit drug activities" was sufficiently particular); United States v. George, 975 F.2d 72, 76 (2d Cir. 1992) (collecting cases in which courts have concluded that description of types of crimes is sufficiently particular); Riley, 906 F.2d at 844 (holding warrant that authorized seizure of "items that constitute evidence of the offenses of conspiracy to distribute controlled substances" was sufficiently particular); United States v. Reed, No. 2:13-CR-29-1, 2013 WL 5503691, at *2 (D. Vt. Oct. 2, 2013) (concluding that warrant that authorized seizure of "any and all evidence of trafficking or possession of controlled substances" was sufficiently particular).[23] The warrant's limitation on copying evidence that related to the "trafficking of narcotics or laundering of drug proceeds" was sufficient under the Fourth Amendment.[24] Ex. U at 12214A, 12264A.

---

[22] Although the defendant has not challenged them, the government notes that FlexiSpy Warrants VIII-XV listed the specific statutes at issue in Attachment A to those warrants.

[23] The defendant's reliance on George in support of his argument is misplaced. See Dkt. No. 263 at 11. There, the warrant limited the categories of information sought by the warrant only to evidence "relating to the commission of a crime." 975 F.2d at 74. That is not this case.

[24] For these same reasons, the Court should reject the defendant's argument that FlexiSpy Warrants I & II failed to adequately specify the offenses. See Dkt. No. 263 at 11 n.6.

The defendant next argues that the warrant did not adequately describe the place to be searched. See Dkt. No. 263 at 11. That is inaccurate. Attachment A to FlexiSpy Warrant III listed 35 FlexiSpy accounts to be searched and listed the specific types of information that agents could copy and review. See Ex. U at 12214A, 12264A. That description meets the Fourth Amendment's requirements. See United States v. Westley, No. 3:17-CR-171 (MPS), 2018 WL 3448161, at *12 (D. Conn. July 17, 2018) (holding that warrants "easily satisf[ied] the second element of the particularity requirement" when they listed "Facebook accounts, identified by user ID number and user name in Attachment A," and went beyond the requirement by "describing specific categories of information," such as activity logs, photo and video uploads, and profile information).

In any event, even if FlexiSpy Warrant III were insufficiently particular, it would be valid under the "all-records exception." Nordlicht, 2018 WL 705548, at *6 (internal quotation marks omitted). "Under that exception, when the criminal activity pervades [an] entire business, seizure of all records of the business is appropriate, and broad language used in warrants will not offend the particularity requirements." Id. (alteration and internal quotation marks omitted); cf United States v. Ulbricht, 858 F.3d 71, 102 (2d Cir. 2017) ("[A] warrant may allow the government to search a suspected drug dealer's entire home where there is probable cause to believe that evidence relevant to that activity may be found anywhere in the residence"). In such circumstances, broad warrants are particularly appropriate for searches related to electronic data. See Ulbricht, 858 F.3d at 102 ("[I]t will often be impossible

---

Those warrants also limited the categories of information sought to evidence of "the trafficking of narcotics or the laundering of drug proceeds." Ex. S at 12137A; Ex. T at 12175A.

to identify in advance the words or phrases that will separate relevant files or documents before the search takes place, because officers cannot readily anticipate how a suspect will store information related to the charged crimes."). Here, the defendant was the leader of the Sinaloa Cartel; criminal activity pervaded his entire organization, and he used the FlexiSpy accounts in furtherance of his crimes. Under these circumstances, the all-records exception justified the search of all the data in the FlexiSpy Accounts.

ii. FlexiSpy Warrant III Did Not Violate Rule 41

The defendant claims that FlexiSpy Warrant III violates Rule 41(b) and Rule 41(e)(2)(C). See Dkt. No. 263 at 13-15. The defendant is incorrect on each of these points; but even if the warrant violated Rule 41, the Court still should not suppress the evidence.

As an initial matter, the defendant argues that the warrant violates the venue provision set forth in Rule 41(b)(6), because FlexiSpy Warrant III was issued by a magistrate judge in the SDNY for electronic data located in the Western District of Washington.[25] See Dkt. No. 263 at 13; Fed. R. Crim. P. 41(b)(6) (identifying circumstances in which "magistrate judge has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy"). This rule, however, did not go into effect until December 2016, long after the FBI obtained the warrant in question on February 16, 2012. See Fed. R. Crim. P. 41(b)(6) advisory committee's note to 2016 amendment. Per the Supreme Court's order accompanying the December 2016 Amendments, those amendments "shall govern in all

[25] As previously noted, see section IV.A. supra, an SDNY magistrate judge issued FlexiSpy Warrants I & II for discs containing FlexiSpy Data, which were located at FBI offices within the SDNY. SDNY Magistrate judges issued FlexiSpy Warrant III and the remaining FlexiSpy Warrants for electronic data located in the Western District of Washington.

proceedings in criminal cases thereafter commenced and, insofar as just and practicable, all proceedings then pending." United States Supreme Court Order of April 28, 2016; see United States v. Mercado, 349 F.3d 708, 711 (2d Cir. 2003) (holding that amendments to Rule 11 need not be applied retroactively). Applying the 2016 Amendment to a 2012 warrant would not be just or practicable, as the rule simply did not exist when the FBI agents applied for, and the magistrate issued, the warrant. See United States v. Deichert, 232 F. Supp. 3d 772, 781 (E.D.N.C. 2017) (concluding that Rule 41(b)(6) does not apply retroactively); see also Landgraf v. Usi Film Prods., 511 U.S. 244, 275 n.29 ("A new rule concerning the filing of complaints would not govern an action in which the complaint had already been properly filed under the old regime, and the promulgation of a new rule of evidence would not require an appellate remand for a new trial."). As such, a motion to suppress based on Rule 41(b)(6) would be retroactive, and the Court should deny it.

In any event, even if applicable, this provision would not foreclose the SDNY magistrate's authority to issue the warrant. Rule 41 does "not modify any statute regulating search or seizure, or the issuance and execution of a search warrant in special circumstances." Fed. R. Crim. P. 41(a)(1). It therefore does not modify the provisions of the Stored Communications Act ("SCA"), see 18 U.S.C. § 2701 et seq., which "regulates search and seizure of electronic evidence." United States v. Scully, 108 F. Supp. 3d 59, 82 (E.D.N.Y. 2015) (internal quotation marks omitted). That statute, which addresses electronic data stored in the possession a "remote computing service," permits "any district court of the United States (including a magistrate judge of such court) that . . . has jurisdiction over the offense being investigated" to issue a warrant for such electronic data. 18 U.S.C. § 2711(2)-(3); see id.

§ 2703(b)(1)(A), (d); Scully, 108 F. Supp. 3d at 83 (stating that SCA permits "nationwide service of search warrants for electronic evidence").

Here, the SDNY magistrate issued FlexiSpy Warrant III for electronic data in the possession of Amazon, which is a remote computing service under the SCA. See 18 U.S.C. § 2711(3) (defining term "remote computing service" to mean "the provision to the public of computer storage or processing services by means of an electronic communications system"). The magistrate judge had jurisdiction over the offense being investigated; at the time, FBI agents and SDNY prosecutors were conducting an investigation into the defendant's violations of 21 U.S.C. §§ 959 and 963, among other crimes. See 21 U.S.C. § 959(d) (describing extraterritorial reach of statute). Accordingly, under the SCA, the SDNY magistrate judge had jurisdiction to issue the warrant for the data located in the Western District of Washington. See Scully, 108 F. Supp. 3d at 83 (concluding that EDNY magistrate had authority to issue warrant for email accounts located in California under SCA).

With respect to Rule 41(e)(2)(C), the defendant claims that the tracking warrant, submitted as part of FlexiSpy Warrant III, "on its face does not identify the 'property to be tracked [or] the magistrate judge to whom it must be returned.'" Dkt. No. 263 at 15. That rule lists certain requirements for a warrant for a tracking device, including that it "must identify the property to be tracked" and "designate the magistrate judge to whom it must be returned." Fed. R. Crim. P. 41(e)(2)(C). The defendant's claims with respect to this rule are meritless.

First, FlexiSpy Warrant III does indicate the property to be tracked; it stated the property to be tracked was "Location Data Contained in the FlexiSpy Accounts Listed in Attachment A," which in turn specifies the 35 accounts from which the FBI agents would obtain the location data. Ex. U at 12262A, 12264A. Thus, the warrant sufficiently identified

the property to be searched. See Westley, 2018 WL 3448161, at *12. Second, while the warrant does not specifically identify the magistrate judge to which it should be returned—instead indicating that the warrant should be returned to the Clerk of Court, see Ex. U at 12262A—to the extent that this language does not comply with Rule, courts have concluded that such minor errors do not justify suppression. See United States v. Turner, 781 F.3d 374, 386 (8th Cir. 2015) (finding that there was no prejudice despite Rule 41 procedural violations such as "[t]he government fail[ing] to designate a judge to which the warrant must be returned"); United States v. Salazar, No. 16-cr-264 (SRN/HB), 2017 WL 1365110, at *8 (D. Minn. Mar. 23, 2017) (stating that "the failure to designate a magistrate judge for return of the warrant does not warrant suppression").

Even if the Court concludes that FlexiSpy Warrant III violated Rule 41, "the Second Circuit has counseled that violations of Rule 41 should not lead to exclusion unless (1) there was 'prejudice' in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule." Scully, 108 F. Supp. 3d at 85 (internal quotation marks omitted). Here, the violations asserted by the defendant are minor and relate to location of the evidence to be searched and seized, the identification the property to be tracked and the name of the magistrate judge to which the warrant should be returned. The alleged errors did not result in any prejudice. The search still would have occurred and the scope would not have changed had these alleged errors been "corrected." At most, a magistrate judge in the in the Western District of Washington would have issued the warrant, rather than a judge in the SDNY. These asserted errors are not grounds for suppression.

C. The CS Consented to the Search for the FlexiSpy Data

Alternatively, for the same reasons set forth in section III.D. supra, the searches of the FlexiSpy accounts were valid under the Fourth Amendment because the CS consented to them. The CS had access to the FlexiSpy accounts as part of his job duties for the defendant. In light of his authority over those accounts, he could lawfully provide consent for the FBI to search them. See Davis, 967 F.2d at 87.

D. The FBI Agents Acted in Good Faith

Assuming that the Court finds that the FBI Agents violated the Fourth Amendment in obtaining the FlexiSpy Data, the Court still should deny the defendant's suppression motion under the good-faith doctrine. The FBI Agents not only acted in good-faith reliance on binding appellate precedent under Davis, they also acted in good-faith reliance upon duly issued search warrants under United States v. Leon, 468 U.S. 897 (1984). Thus, suppression here would serve no deterrent purpose. The Court should deny the defendant's motion as to the FlexiSpy Data.

i. The Good-Faith Doctrine under *Davis* and *Leon*

As noted above, see section III.E. supra, "[a] violation of the Fourth Amendment does not necessarily result in the application of the exclusionary rule." United States v. Romain, 678 F. Appx. 23, 25 (2d Cir. 2017) (alteration in original; internal quotation marks omitted). The "sole purpose" of the exclusionary rule "is to deter future Fourth Amendment violations," Davis, 564 U.S. at 236-37, and for this reason the Supreme Court has "limited the rule's operation to situations in which this purpose is . . . most efficaciously served," id. at 237 (internal quotation marks omitted). Thus, when a search is conducted in "strict compliance with then-binding Circuit law" suppression is not appropriate. Id. at 239-40. Similarly, under

Leon, exclusion of evidence is inappropriate "when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope," id. at 920, because "an officer is [not] required to disbelieve a judge who has just advised him, by word and by action, that the warrant he possesses authorizes him to conduct the search he has requested," Massachusetts v. Sheppard, 468 U.S. 981, 989-90 (1984).

Nevertheless, as to this latter application of the good-faith doctrine, evidence obtained pursuant to a warrant should be excluded in any of the following circumstances: "(1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; [or] (4) where the warrant is so facially deficient that reliance upon it is unreasonable." United States v. Moore, 968 F.2d 216, 222 (2d Cir. 1992) (alteration in original) (citing Leon, 468 U.S. at 923). These exceptions reflect the general rule that, "[t]o trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." Herring v. United States, 555 U.S. 135, 144, (2009).

ii. The FBI Agents Acted in Good-Faith Reliance on Binding Appellate Precedent

When the FBI agents copied the FlexiSpy Data prior to the execution of FlexiSpy Warrants I & II, they acted in good-faith reliance upon the Supreme Court's decisions in Soldal and Hicks that a Fourth Amendment seizure does not occur unless law enforcement action interferes with an individual's possessory interest. See Soldal, 506 U.S. at 61; Hicks, 480 U.S. at 324. Indeed, as the Second Circuit had not yet decided its now-vacated decision

in Microsoft at the time of the searches in 2012, there was no circuit authority calling that principle into question. The FBI agents also reasonably relied upon the Second Circuit's decision in Martin, which permitted them to seize temporarily evidence based upon probable cause to avoid loss or destruction of it while they obtained a search warrant. See United States v. Martin, 157 F.3d at 53. Although the good-faith standard is objective—and the subjective intent of the agents and prosecutors at the time is not relevant in this analysis, see Davis, 564 U.S. at 237; Leon, 468 U.S. at 922 n.23—there is no doubt that they, in fact, considered these principles at the time. FlexiSpy Warrants I & II both cited Gorshkov in support the warrant applications to the Court, arguing that the court in that case had approved "a similar method, under analogous circumstances, to collect data in order to execute a search warrant." Ex. S at 12148A; Ex. T at 12186A. Gorshkov, in turn, discusses the same principles articulated in Soldal, Hicks and Martin. Thus, the FBI agents acted in objectively reasonable reliance on those cases in copying the FlexiSpy Data prior to executing FlexiSpy Warrants I & II.

Moreover, as noted above, at the time the FBI copied the data prior to obtaining FlexiSpy Warrants I & II, (1) Verdugo-Urquidez had established that foreign citizens could not invoke the Fourth Amendment, see section II supra; and (2) Davis II had articulated the two-part test to evaluate a third-party's consent to an area over which he has common authority with the defendant, see section III.D. supra. The FBI agents thus acted in good-faith reliance upon this precedent in concluding they did violate the Fourth Amendment by copying the data.

iii. The FBI Agents Acted in Good-Faith Reliance on FlexiSpy Warrants I-III

The FBI agents also acted in good-faith reliance on the duly executed warrants. With respect to FlexiSpy Warrants I & II, the government clearly set forth in its affidavits in

support thereof that it had copied the data to discs prior to seeking the warrants. See Ex. S at 12148A; Ex. T at 12186A. Two separate magistrate judges signed the warrants authorizing the searches of those discs. The FBI agents were entitled to rely on those warrants.

Similarly, with respect to FlexiSpy Warrant III, the issuing magistrate judge found that warrant sufficiently particular based on the description of the offenses and the property in the warrant. Indeed, three different magistrate judges concluded that identical language in other FlexiSpy Warrants was sufficiently particular. See Exs. U-Y. The FBI Agents were not required to second-guess those determinations. In any event, if the descriptions of the types of crimes—"trafficking of narcotics or the laundering of drug proceeds," Ex. U at 12214A, 12264A—in the warrant form and Attachment A for FlexiSpy Warrant III were not sufficiently particular, the underlying application and affidavit, which cited the specific statutes at issue, clarified the scope of the warrant. See Romain, 678 F. Appx. at 25-26 (applying good-faith doctrine, where "the supporting documents but not the warrant itself detailed the relevant criminal offenses being investigated and described the relationship between those crimes and the search sought to be conducted"). The FBI agents thus were justified in acting based upon this warrant.

Likewise, as to the alleged Rule 41 violations, six different SDNY magistrate judges concluded that they had the authority to issue a search warrant for electronic data in the Western District of Washington. The FBI agents had no reason to conclude otherwise. "To the extent that a mistake was made in issuing the warrant, it was made by the magistrate judge[s], not by the executing officers, and the executing officers had no reason to suppose that a mistake had been made and warrant was invalid." United States v. Kim, No. 16-CR-191 (PKC), 2017 WL 5256753, at *6 (E.D.N.Y. Nov. 10, 2017) (internal quotation marks omitted).

"A magistrate judge's mistaken belief that she had jurisdiction, absent any indicia of reckless conduct by the agents, does not warrant suppression." Id. (internal quotation marks omitted). "Furthermore, there is no evidence that any failure by the FBI to understand the intricacies of the jurisdiction of federal magistrates was deliberate . . . ." Id. (internal quotation marks omitted). Accordingly, assuming that FlexiSpy Warrant III violated Rule 41, suppression is not justified. See id. (concluding that good-faith doctrine applied to NIT warrant, which authorized agents to access a private computer in another jurisdiction).

E. Under the Corrected Affidavit Doctrine, the Court Should Not Suppress the FlexiSpy Data

Without any supporting analysis, the defendant argues that the evidence obtained pursuant to the remaining FlexiSpy Warrants should be suppressed as the fruit of the poisonous tree, if the Court concludes that FlexiSpy Warrants I-III violated the Fourth Amendment. See Dkt. No. 263 at 15. Suppression of the evidence derived from the remaining warrants, though, is far from automatic if the Court concludes that FlexiSpy Warrants I-III, or any one of them, were invalid. To the contrary, under the corrected-affidavit doctrine, suppression would not be appropriate.

"When an application for a search warrant includes both tainted and untainted evidence, the warrant may be upheld if the untainted evidence, standing alone, establishes probable cause." Laaman v. United States, 973 F.2d 107, 115 (2d Cir. 1992). "Where improper material is included in a warrant application, the court should disregard that information and 'determine whether the remaining portions of the affidavit would support probable cause to issue the warrant.'" United States v. Jones, No. 3:13-CR-2 MPS, 2014 WL 1154480, at *9 (D. Conn. Mar. 21, 2014) (quoting United States v. Canfield, 212 F.3d 713,

718 (2d Cir. 2000)). "If the corrected affidavit supports probable cause, the inaccuracies were not material to the probable cause determination and suppression is inappropriate." Id. (internal quotation marks omitted). "The ultimate inquiry is whether, after putting aside erroneous information and material omissions, 'there remains a residue of independent and lawful information sufficient to support probable cause.'" Canfield, 212 F.3d at 718 (quoting United States v. Ferguson, 758 F.2d 843, 849 (2d Cir. 1985)).

Here, the initial probable cause determination in FlexiSpy Warrant I was based upon information from the CS. The government included that CS information in each of the subsequent warrant affidavits, along with other corroborating information, such as information related to capture operations and other sources of information. See, e.g., Ex. T at 12181A-12186A. Over time, the government added additional CS information to the warrants based on further conversations that the CS had with the defendant's co-conspirators. See, e.g., GG 13209A-13242AA. In addition, later FlexiSpy Warrants cited communications gathered pursuant to earlier FlexiSpy Warrants, including communications of the defendant regarding his drug trafficking and attempts to evade law enforcement detection. See, e.g., id. But even if the Court struck as tainted all of the communications derived from FlexiSpy Warrants I-III from the later warrants (or if it struck the information from one or some combination of those warrants), the CS information, other source information and corroborating evidence still would remain. That information, on its own, would establish probable cause in each of the FlexiSpy Warrants to search for the FlexiSpy Data. This is not conjectural. An SDNY magistrate judge issued FlexiSpy Warrant I based solely on CS information. Thus, under the corrected affidavit doctrine, the evidence derived from any warrants that comported with the Fourth Amendment

is not tainted as fruit of the poisonous tree. The Court should deny the defendant's motion in that regard.

V. Partial Sealing is Appropriate

Pursuant to the protective order in this case, the government respectfully requests permission to submit this brief partially under seal. See Dkt. No. 57 ¶ 8. The government designated the MLAT requests for the Dutch Calls and the FlexiSpy Warrants as "Protected Material" under the protective order to protect the identities of the confidential sources and the sensitive law enforcement techniques discussed therein. See Dkt. No. 57 ¶ 1. Portions of this brief refer to that material, and the government seeks to seal those portions to protect the identity of the confidential sources and avoid disclosure of those techniques. Notably, although the CS is not identified by name herein, the defendant's criminal associates likely could use the information described herein to identify the CS.

Thus, partial sealing is warranted because of the concerns regarding the safety of potential witnesses and their families, and the danger posed by disclosing the potential witnesses' identities and their cooperation with the government. See United States v. Amodeo, 44 F.3d 141, 147 (2d Cir. 1995) (need to protect integrity of ongoing investigation, including safety of witnesses and the identities of cooperating witnesses, and to prevent interference, flight and other obstruction, may be a compelling reason justifying sealing); see Feb. 5, 2018 Mem. & Order Granting Gov't Mot. for Anonymous and Partially Sequestered Jury, Dkt. No. 187 at 2-3 (concluding that defendant's actions could pose risk of harm to cooperating witnesses). As the facts set forth herein provide ample support for the "specific, on the record findings" necessary to support partial sealing, Lugosch v. Pyramid Co., 435 F.3d 110, 120 (2d. Cir. 2006), the government respectfully requests that the Court permit the government to file

this opposition to the defendant's suppression motions partially under seal. Should any order of the Court regarding this application describe the sealed information in question with particularity, rather than in general, the government likewise requests that those portions of the order be filed under seal.

CONCLUSION

For the foregoing reasons, the Court should deny the defendant's motions to suppress in their entirety.

Dated: Brooklyn, New York
July 30, 2018

Respectfully submitted,

RICHARD P. DONOGHUE
Acting United States Attorney
Eastern District of New York

ARTHUR G. WYATT, CHIEF
Narcotic and Dangerous Drug Section
Criminal Division
U.S. Department of Justice

OF COUNSEL:
BENJAMIN G. GREENBERG
United States Attorney
Southern District of Florida